APPENDIX D

Privacy Impact Assessments: Jurisdictional Report for the United States of America

CONTENTS

The Legislative and Policy Framework

A complex body of law (constitutional, tort and statutory) governs the collection, processing and disclosure of personally identifiable information in the United States. The main federal laws governing privacy protection within the federal public sector are:

- The *Privacy Act* of 1974, 5 U.S.C. § 552a applies fair information principles to the personal information held by federal government agencies.
- *The Computer Matching and Privacy Protection Act,* 5 U.S.C. 552a(o) describes the manner in which computer matching involving Federal agencies should be performed
- The *Driver's Privacy Protection Act*, 18 U.S.C. 2721-2725 prohibits the release and use of certain information from state motor vehicle records.
- The *Computer Security Act*, Public Law 100-235 establishes a minimum acceptable security practices for federal information systems and requires the creation of computer security plans, and the appropriate training of system users where the systems house sensitive information.
- The *Electronic Communications Privacy Act* , 18 U.S.C. § 2510, sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications.
- *The Electronic Government Act* of 2002, 44 U.S. § 101, establishes new agency requirements, including PIAs, for the development of e-government initiatives.

There is no comprehensive privacy protection law governing the private sector. However, the main federal provisions are:

- The *Federal Trade Commission Act*, 15 U.S.C. § 41, et seq., empowers the FTC to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.
- Title V of the *Gramm-Leach Blighly Act*, 15 U.S.C. § 6801, et seq., enacted in 1999, contains privacy provisions relating to consumers' personal financial information.
- The *Children's Online Privacy Protection Act* 15 U.S.C. § 6501, et seq., was enacted in 1998 to protect the personal information of children under the age of 13 that is collected online.

  The *Identity Theft Act*, 18 U.S.C. § 1028, 1028(a)(7) made it a federal crime to knowingly transfer or use, "without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."
- The *Cable Communications Policy Act* of 1984 47 U.S.C. § 551, restricts the collection, maintenance, and dissemination of subscriber information.
- The *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) 42 U.S.C. § 1320d, et seq., and regulations issued by the Department of Health and Human Services (HHS) create standards to protect the privacy of individuals' personal health information.
- The *Fair Credit Reporting Act* (FCRA) 15 U.S.C. § 1681, et seq., first enacted in 1970 and most recently amended in 1996, is designed to promote the accuracy and ensure the privacy of the sensitive financial information contained in consumer credit reports.

- The *Federal Videotape Privacy Protection Act*, 18 U.S.C. § 2710, enacted in 1988, addresses information about consumers' videotape purchases and rentals.

Tort law also plays a more important role in the United States than in other countries, as does the 200 year old history of interpretation of the "unreasonable search and seizure" clause within the 4th Amendment of the federal Constitution. There are also an enormous number and range of statutes at the various state levels. Three legislative provisions are especially relevant for the conduct of PIAs within the federal government.

The first and most general is the *Administrative Procedure Act* of 1946, which governs the general method by which federal agencies may propose and establish regulations. The basic purposes of the APA are:

(1) to require agencies to keep the public informed of their organisation, procedures and rules;
(2) to provide for public participation in the rulemaking process;
(3) to establish uniform standards for the conduct of formal rulemaking and adjudication;
(4) to define the scope of judicial review.

Most federal agencies have developed rules through "informal rulemaking" including: Publication of a "Notice of Proposed Rulemaking" in the Federal Register; opportunity for public participation by submission of written comments; consideration by the agency of the public comments and other relevant material; and publication of a final rule not less than 30 days before its effective date, with a statement explaining the purpose of the rule.

Secondly, the *Privacy Act* of 1974 establishes the basic statutory "fair information principles" for federal agencies and obliges the publication of a Systems of Record Notice (SORN) when most new personal information systems are established. All Federal agencies are required to publish in the Federal Register each system of records when the system is established or changed. These notices include the following: Name and location of the system; Categories of individuals on whom records are maintained in the system; Categories of records maintained in the system; Each routine use of the records contained in the system, including categories of users and purpose of such use; Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; Title and business address of the agency official responsible for the system of records; Agency procedures whereby an individual can be notified at his or her request if the system of records contains a record pertaining to him or her; Agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her contained in the system of records, and how he or she can contest its contents; and Categories of sources of records in the system. There are exemptions for systems established for national security reasons.[1]

Thirdly, the *Electronic Government Act* of 2002 states that each federal agency shall undertake a PIA "before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information." Agencies are to ensure review by the Chief Information

[1] *The Privacy Act* of 1974 (5 U.S.C. § 552a). See also: Office of Management and Budget, Instructions for complying with the President's Memorandum of May 14, 1998 "Privacy and Personal Information in Federal Records" at: http://www.whitehouse.gov/omb/memoranda/m99-05-b.html.

Officer, or equivalent official, as determined by the head of the agency; and "if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." This requirement may be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment."[2] This legislation was designed to supplement the broader requirements within the *Privacy Act*.

Responsibility for providing guidance on the interpretation of privacy protection policy in the federal government rests with the Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB), the agency within the Executive Office of the President responsible for developing the President's budget proposals and for the central coordination and oversight of a range of procurement, financial management, information and regulatory policies. It is seen as "central agency" for the purposes of this study.

The analysis begins with the history and context of PIAs in the United States, and describes the general process established under the *Electronic Government Act* of 2002 for the conduct of PIAs in the federal government as a whole. It then discusses the approaches of three agencies (the Internal Revenue Service {IRS}, the Department of Homeland Security {DHS} and the US Postal Service {USPS}), whose experiences have been distinctive. The case study concludes with some general lessons about the conduct of PIAs in the United States, and their applicability to the UK.

History and context of PIAs in the United States

It is impossible to gauge the extent of the use of PIAs within the American private sector, although it is probable that assessments of privacy implications have been an integral part of new product and service review for many companies for a long time. They tend to be internal, and often proprietary, analyses whose final products are rarely made public. PIAs must also be considered in the light of a whole range of self-regulatory mechanisms, including codes of practice, certification tools, privacy notices and privacy seals, which have spread throughout the US commercial sector in recent years.[3] Just because there are few instruments called PIAs published within the US corporate sector, does not mean that equivalent risk assessments are not performed.

Whereas there is an unknown number of PIAs in the US private sector, it can be asserted that there are very few examples at the state level, although California's Office of Privacy Protection, one of the only oversight bodies[4] with responsibility for privacy protection, is beginning to see PIA methodology as a part of their best practices recommendations for state authorities. For the first time, the use of PIAs is defined as a task within California's plan for information technology. By autumn 2007, the State Privacy Officer, in consultation with the State Information Security Office is supposed to develop a methodology and a set of tools that departments can use to "self assess the

[2] The Electronic Government Act of 2002, 44 USC 101.
[3] Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006), ch. 6.
[4] Although this organisation fulfils some "oversight" functions, such as taking complaints, it also has a "central agency" role and is not independent of the administrative arm of the California State government.

privacy impact of proposed new and major modifications to existing IT systems that contain personal information."[5]

Thus the development of PIAs in the United States is principally confined to the activities of the federal government. Their history dates to the mid-1990s when the IRS began to require them for certain large projects, and issued a set of PIA guidelines in 1996 (later revised). The main impetus, however, was provided by the enactment of the *Electronic Government Act* of 2002. The central purpose of this law is to improve the management and promotion of electronic government services through the Internet. According to the presidential signing statement: "This legislation builds upon my Administration's expanding e-government initiatives by ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programmes, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services, consistent with the reform principles I outlined on July 10, 2002, for a citizen-centered, results-oriented, and market-based Government."[6]

The PIA provisions did not generate a lot of attention at the time, even though it was obvious that they would have implications beyond the "e-government" context. They were seen by the privacy advocacy community as a way to push for some incremental improvements to federal privacy protection policy, given their calculation that oversight by a more general privacy protection agency was not considered feasible, nor enactable.[7] Within a complex landscape of privacy protection laws which tend to fix privacy problems in a pragmatic and reactive manner after they have occurred,[8] these PIA provisions do stand out as comparatively forward-looking. Their execution is, however, variable and very much dependent on factors peculiar to individual agencies.

We will review the general process for conducting PIAs within federal agencies, as a whole, and then focus more specifically on three agencies which have developed more distinctive PIA methodologies (the IRS, the DHS and the US Postal Service).

The American PIA Process

PIAs must analyse and describe: what information is to be collected including the nature and the source; why the information is being collected; the intended use(s) of the information; with whom the information will be shared, such as another agency for a specified programmatic purpose; what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorised uses), and how individuals can grant consent; how the information will be secured through administrative and technological controls; and whether a system of records is being created under the *Privacy Act*.

<u>The Tools</u>

[5] http://www.cio.ca.gov/pubs/StrategicPlan.html
[6] President signs E-Government Act, http://www.whitehouse.gov/news/releases/2002/12/20021217-5.html.
[7] Interview with Ari Schwartz, Center for Democracy and Technology (CDT), August 10, 2007.
[8] See, for example, the arguments about the American policy style in Colin J. Bennett, *Regulating privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

Under the *Electronic Government Act*, a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice would be provided to individuals and how the information will be secured. Seven months after the statute's operative date, the Office of Management and Budget (OMB) issued guidelines on how PIAs should be conducted.[9] The general presumption is that responsibility for PIA compliance is delegated to individual agencies. Separate guidelines (from those of the OMB) have been prepared by the Privacy Office of the DHS[10], by the Privacy and Civil Liberties Office within the Department of Justice,[11] by the US Postal Service[12] and by the IRS[13] among others.

Completion of PIAs

Who Participates in the PIA?

It is generally presumed that PIAs in the federal government will be conducted by relevant programme managers in consultation with experts in the areas of information technology, IT security, records management and privacy. Although the OMB guidance allows considerable discretion, it is clear that the *Electronic Government Act's* privacy provisions were intended to make systems development a multidisciplinary effort.[14]

When and under what circumstances are PIAs conducted?

The Electronic Government Act requires agencies to conduct a PIA before: "developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government)." The OMB guidance provides some examples of the kinds of system changes that might create new privacy risks:

- when converting paper-based records to electronic systems;
- when functions applied to an existing information collection change anonymous information into information in identifiable form;
- when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralised, matched with other databases or otherwise significantly manipulated;

[9] OMB**,** Electronic Government Act Section 208 Implementation Guidance, http://www.whitehouse.gov/omb/memoranda/m03-22.html. This delay has been interpreted as signalling a lack of commitment to the statute. Kenneth A Bamberger and Deidre Mulligan, "Privacy Decision-Making in Administrative Agencies," Chicago Law Journal forthcoming.
[10] At: http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.
[11] At: http://www.usdoj.gov/pclo/pia.htm.
[12] At: http://www.usps.com/privacyoffice/pia.htm.
[13] At: http://www.irs.gov/irm/part11/ch02s01.html.
[14] As quoted by OMB staff in Jason Miller, "Serious about Privacy," *Government Computer News*, May 17, 2004 at: http://www.gcn.com/print/23_11/25917-1.html.

- when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources;
- when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting e-government initiatives; development of this cross agency IT investment;
- when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

The guidance also specifies the conditions under which PIAs may *not* be required: "when IT systems do not collect or maintain information in identifiable form about members of the general public; where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g. questions or comments) or obtaining additional information; for certain national security systems; when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the *Privacy Act*; when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes; when agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form; and for minor changes to a system or collection that do not create new privacy risks. Agencies must also update their PIAs to reflect "changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form."

Agencies should commence a PIA when they begin to develop a new or significantly modified IT system, and its depth and content should be "appropriate for the nature of the information to be collected and the size and complexity of the IT system." A distinction is also made between: 1) "major information systems" the PIAs for which should reflect more extensive analyses of: the consequences of collection and flow of information, the alternatives to collection and handling as designed, the appropriate measures to mitigate risks identified for each alternative and, the rationale for the final design choice or business process; 2) "routine database systems" where a more standardised approach such as a checklist or template is appropriate. In both cases agencies must consider the information "life cycle" and evaluate how information handling practices at each stage may affect individuals' privacy.

Review and Approval of PIAs

The E-Government legislation and the OMB Guidance specifies that agencies must also ensure that the PIA document be approved by a "reviewing official" (the agency Chief Information Officer or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA). Agencies are given wide latitude under the Act to assign responsibilities for the conduct of PIAs.

OMB is the major central budget coordination agency within the federal government. Thus, incentives for the preparation of PIAs are built into the annual budget approval

cycle and agencies must have privacy compliance documentation in place before going to OMB for funding. It is, however, difficult to ascertain whether budgets are indeed sent back for review because the PIA was insufficient or incomplete because these internal budget decisions are rarely made public. PIAs might also be triggered by the requirement within the *Federal Information Security Management Act* (FISMA) that agencies must report annually to the OMB and to Congress on the effectiveness of the agency's security programmes. From time to time, there have also been oversight by the Governmental Accountability Office[15] and by certain Congressional committees.[16]

External Consultation

There is no provision in either the Electronic Government Act, or the accompanying OMB Guidance for any external stakeholder consultation on draft PIAs. Rarely, therefore, are those outside the agency asked to comment or provide any input before a PIA is published.

The only notable exception where external consultation occurred in advance of PIA publication was as a result of HSPD-12, the Presidential directive mandating a common identification standard for federal employees and contractors.[17] This directive mandated the National Institute of Standards and Technology (NIST) to promulgate a Federal standard for secure and reliable forms of identification. The widespread implications of this standard prompted a full-day meeting, hosted by OMB, with privacy and civil liberties advocates before the PIA process was concluded. The meeting was reportedly a valuable, but rare, occasion when outside input was sought.[18]

Public Availability and Accountability

In contrast to PIAs in other countries, there is a requirement that the resulting documentation should be made public, although agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement efforts or competitive business interests). Such information is meant to be handled in a manner consistent with the *Freedom of Information Act* (FOIA).

Many agencies now post PIAs on their respective websites. Hence, and after just five years in operation, there are now a large number of PIAs, of varying length and substance, which are published and available for review. These published PIAs are for the: Department of Homeland Security[19]; Internal Revenue Service[20]; US Postal Service[21]; Department of Transportation[22]; Department of Labor[23]; Department of

[15] US Governmental Accountability Office, *Homeland Security: DHS Privacy Office has Made Progress but faces Continuing Challenges*, Statement by Linda Koontz, Director Information Management Issues, GAO-07 1024T at: http://www.gao.gov/new.items/d071024t.pdf.
[16] Particularly by the Subcommittee on Commercial and Administrative Law of the House Judiciary Committee.
[17] At: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.
[18] Interview, Ari Schwartz, August 10th, 2007
[19] Department of Homeland Security at: http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#10.
[20] Internal Revenue Service at: http://www.irs.gov/privacy/article/0,,id=122989,00.html.
[21] US Postal Service at: http://www.usps.com/privacyoffice/pialist.htm.
[22] Department of Transportation at: http://www.dot.gov/pia.html.
[23] Department of Labor at: http://www.dol.gov/cio/programmes/pia/mainpia.htm

State[24]; Department of Justice[25]; Department of Health and Human Services[26]; Department of Education[27]; Bureau of the Census[28]; and several others.

These requirements for publicity should also be seen in conjunction with the *Privacy Act* requirement for federal agencies to publish a Systems of Records Notice (SORN) in the *Federal Register* for each agency system that collects more than one record that contains information about an individual and is designed to be retrieved by name or other personal identifier. The SORN is typically a briefer statement preceding a more thorough PIA.

Individual Agency Experiences

There is no easy conclusion about the impact of PIAs within the US federal government because the models vary. The experience of three agencies, the IRS, the DHS and the USPS represent subtly different approaches to PIA development and implementation.

The Internal Revenue Service (IRS)

The IRS was one of the first agencies anywhere in the world to develop PIAs, attributable to the fact that in 1993, as a result of some highly publicised abuses of taxpayer information, the agency decided to institutionalise an Office of the Privacy Advocate. The IRS has, therefore, had a lengthy experience with conducting PIAs both before and since the Electronic Government Act was passed. In 2000, its PIA process was endorsed as a best practice by the Federal Chief Information Officer's Council.[29]

Within the IRS, the PIA process is explicitly designed to guide business owners and system developers in evaluating privacy risks through the stages of system development. Owners of new systems, systems under development, or systems undergoing major modifications are required to complete a PIA, but there is no pre-screening tool as in DHS. The purpose of the PIA is to identify privacy risks in the system and to limit the information collected and used to only what is relevant to achieve a legitimate business purpose. The business Owner and system Developer must initiate the PIA in the early stages of the development of a system and complete it as part of the system's required Enterprise Life Cycle review.[30]

Review of PIAs within the agency is the responsibility of the Director of the Office of Privacy, formally called the Office of the Privacy Advocate. This office was established in 1993 and developed its own set of Privacy Principles, disseminated in May 1994. This office reserves the right to request that a PIA be completed on any existing system that they determine may have privacy risks. It is responsible for the development of policies to protect taxpayer and IRS employee privacy and ensures that they are integrated into all IRS practices and policies. It also answers questions on PIA procedures, provides training, and serves as an agency resource on privacy issues. Business owners and system developers submit the completed PIA to the Privacy Office for analysis, which

[24] Department of State at: http://foia.state.gov/piaOnline.asp.
[25] Department of Justice at: http://www.usdoj.gov/pclo/pia.htm.
[26] Department of Health and Human Services at: http://www.hhs.gov/foia/.
[27] Department of Education at: http://www.ed.gov/notices/pia/index.html.
[28] Bureau of the Census at: http://www.census.gov/po/pia/.
[29] Federal Chief Information Officer's Council, Internal Revenue Service Model Information Technology Privacy Impact Assessment, February 25, 2000 at: http://www.cio.gov/Documents/pia_for_it_irs_model.pdf.
[30] Part 11., "Communications and Liaison," IRS, at: http://www.irs.gov/irm/part11/ch02s01.html.

reviews the completed PIA to identify privacy risks and to ensure only relevant and necessary information is collected and used. There is then an attempt to reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached, the unresolved issues will be presented to the Chief Information Officer for his decision. The Business owner and system developer also are expected to conduct life cycle review of systems to ensure satisfactory resolution of identified privacy risks.[31]

It appears, therefore, that IRS places more stress on the *process*, than on the final privacy impact *statement*. According to the relevant guidance material: "Privacy issues must be addressed when systems are being developed or updated, and privacy protections must be integrated into the life cycle of these automated systems. The vehicle for addressing privacy issues in a system is the Privacy Impact Assessment (PIA). The PIA process also provides a means to monitor compliance with applicable laws and regulations governing taxpayer and employee privacy."[32]

The Department of Homeland Security (DHS)

The DHS Privacy Office is the first statutorily required Privacy Office at any federal agency. Its mission is to minimise the impact on the individual's privacy and oversee the operation of Section 222 of the Homeland Security Act, the *Privacy Act* of 1974, the Freedom of Information Act, the Electronic Government Act of 2002 and other Executive Orders, court decisions and DHS policies that protect the collection, use, and disclosure of personal information. It operates under the direction of the Chief Privacy Officer (CPO), who is appointed by the Secretary. With respect to the activities of the DHS, the Privacy Officer also has authority under Section 222 of the Homeland Security Act of 2002 to require PIAs. Because of this provision, PIAs tend to be defined and used more broadly in the DHS than in other federal agencies.[33]

The DHS has adopted a Privacy Threshold Analysis (PTA) instrument, a simple five-page form designed to determine whether a PIA will be required.[34] This analysis could lead to one of two outcomes: a determination that this is not a Privacy Sensitive System because it contains no personally identifiable information; or, it is a Privacy Sensitive System. If the latter, there might be a determination that the PTA is sufficient, or that it is a national security system or human resources system and therefore exempt from the Electronic Government Act, or that it is a legacy system and no changes have been made and thus a PIA is also not required. PTAs have been conducted on all 735 systems within the Department of Homeland Security.[35]

In the DHS, if the PTA indicates that a PIA is necessary, then they are performed normally by the programme manager in coordination with the Information security person. Drafts are prepared, circulated internally and normally reviewed by legal counsel. This is normally an iterative process that can last 4-6 weeks. The document triggers an internal conversation about privacy practices.[36] The draft is then reviewed by the Office of the Director of Privacy Compliance, which will typically provide comments. The vast majority of PIAs do go back to the programme manager for more information and clarification. If the various issues are not addressed, then face-to-face meetings are

[31] http://www.irs.gov/irm/part11/ch02s01.html.
[32] Ibid.
[33] Interview, Rebecca Richards, Director of Privacy Compliance, DHS, August 9, 2007.
[34] http://www.dhs.gov/xlibrary/assets/privacy/DHS_PTA_Template.pdf.
[35] Interview, Rebecca Richards, Director of Privacy Compliance DHS, August 9, 2007.
[36] Interview, Rebecca Richards, DHS, August 7, 2007.

arranged. At the end of the process, the CPO signs off on all PIAs, and will frequently request further changes at this stage. The programme is not allowed to go operational until the CPO has signed off. However, there are a large number of legacy systems which predated the creation of the DHS, which are far more difficult to evaluate. The vast majority of DHS PIAs are published on the DHS website.

The DHS Privacy Office does hold some public workshops at which PIA process may be discussed in the context of the larger debates about the relationship between privacy and homeland security. There is also a DHS Data Privacy and Integrity Advisory Committee which advises the Secretary and the CPO on programmatic, policy, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues. This committee includes representatives from the private sector, academia and the non-governmental organisation sector.

The United States Postal Service (USPS)

The U.S. Postal Service has access to an enormous amount of highly sensitive information - home addresses, credit card numbers, stop-mail orders, change of address forms, the magazines people read and the catalogs from which they order. It is also one of the most trusted organisations in the United States. Significant attention to privacy issues within the USPSS was attributable again to the appointment of a Chief Privacy Officer in 2001, in this case Zoe Strickland who began to re-examine the organisation's Systems of Records and the data flows within the agency. Ms. Strickland helped put together for project managers a full "business impact assessment" process that examines a wide range of potential issues, including privacy and security impact assessments.

The USPS “voluntarily complies” with the Electronic Government Act of 2002. The Postal Service’s PIAs are known as Business Impact Assessments (BIA). They are required for all IT systems, both customer and employee. Separate guidance has been issued in the form of BIA template guidance in short and long forms, both of which go some way beyond the OMB guidance. They appear also to be a good deal broader than a legislative compliance checklist. To quote: “The BIA addresses all privacy and security requirements, including ensuring privacy compliance, determining the sensitivity and criticality of the system, and developing the appropriate security plan. The BIA has long been postal policy, and is required for all IT systems, including those containing customer or employee information.”[37]

According to Strickland, the process involves five steps:

1) Develop a questionnaire. Each questionnaire should solicit information about a system under development, addressing plans for privacy and security. It also should capture, assess and drive data practices;
2) Define the scope. The assessment should cover all systems within a particular programme, as well as all technologies being used to collect, create or manage information;
3) Establish the schedule. The agency should plan when work on the assessment should start and be completed;

[37] http://www.usps.com/privacyoffice/pia.htm.

4) Determine roles and accountability. Employees should know what is expected of them and who will sign off on the finished assessment;

5) Define how the process works. Each objective should be clearly identified and the PIA process, including approach to risk management, should be easily repeatable.[38]

Lessons Learned from the United States of America

The differences between American and UK data protection policy as well as larger variations in the institutional and administrative culture suggest that there might be few lessons, positive or negative, which usefully can be drawn from the American experience. Privacy laws have emerged pragmatically, reactively and according to the different needs of individual sectors. The overall picture, therefore, has been described as "fragmented, incomplete and discontinuous."[39] American PIA policy needs, therefore, to be evaluated according to US standards, rather than those of countries with comprehensive data protection laws overseen and administered by data protection or privacy agencies with dedicated responsibilities for these issues. Within those parameters, PIAs have stood out as one of the more positive aspects of American privacy protection policy within the last ten years.

Several conclusions about their implementation can be reached from this brief survey.

- The legislative mandate is peculiar in comparative context. It produces a significant number of PIAs, but obviously of variable quality. There is a tendency in some agencies to treat PIAs as things they have to do, rather than things they should do to mitigate risk.
- The presence and type of privacy infrastructure within an agency is probably the most important influence on the successful conduct of PIAs.
- The publication of PIAs contributes to transparency. But the lack of prior consultation with external stakeholders can harm their perceived legitimacy.
- The accountability established within the PIA and SORN frameworks tend to rely on outmoded conceptions of a "system of records" which may not be sufficiently sensitive to the fluid and interactive realities of contemporary data flow environments.

The Legislative Mandate

There is no other example of a national jurisdiction where PIAs are mandated by statute across an entire governmental and administrative system. This mandate produces a significant incentive to produce the relevant documentation as part of the annual budget review cycle. The mandate forces agencies to consider their compliance with the relevant privacy principles within the *Privacy Act*.

Statutory mandates, however, raise the question of whether agencies complete these reviews because they have to, or because it is in their more general interests to mitigate

[38] Jason Miller, "Serious about Privacy." *Government Computer News*, May 17, 2004 at: http://www.gcn.com/print/23_11/25917-1.html.

[39] Robert Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993). See also: Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

privacy risks. Former OMB administrator for e-government and IT, Karen Evans has remarked that PIAs should not just be a check box to OMB to say 'we've done it' but a methodology to think seriously about how they will use citizens' data and incorporate that thinking as they plan new systems and upgrades.[40] There is, however, the danger that statutory compulsion produces a "checklist" approach. The legislative mandate can produce a mentality that PIAs are merely statements, just one more piece of documentation that needs to be in place during the annual budget review process.

Furthermore, the demand for effective and comprehensive PIAs can only be achieved with sufficient staffing resources, and this creates delays. For example, a Governmental Accountability Office Report on the work of the DHS Privacy Office noted some significant progress in the incorporation of privacy management into the Department, as well as the increase in the number of PIAs that had been produced since its inception. It also stressed the challenges in producing PIAs and SORNs in a timely fashion, especially as they relate to the existing legacy systems within the Department.[41] One can only infer that similar or greater challenges are faced in Departments with fewer privacy staff.

The Presence and Type of Privacy Infrastructure

PIA rules have been applied "highly inconsistently across agencies, and even between programmes" according to Ken Bamberger and Deidre Mulligan.[42] Their case studies of PIAs within the Department of State and the DHS tend to support an overall conclusion that PIAs are more likely to be conducted more seriously, and thus have an impact on agency culture, if there is a "privacy infrastructure" – comprised of specialised personnel who not only know about the law and the technology, but can forcefully articulate the larger ethical and moral questions. There seems to be a common agreement that the privacy infrastructure within agencies such as the IRS, DHS and USPS has the potential to institutionalise meaningful PIA compliance. This experience supports the proposition that it is often better to have the privacy rationale articulated from within, than from without. It allows the agency experts to scrutinise PIAs before they go out of the door. But Bamberger and Mulligan also caution that such compliance is highly contingent on the leadership skills of a forceful CPO. In many respects, these conclusions echo well-established generalisations about the successful implementation of any privacy protection policy or law.[43] While the expertise of a privacy office is essential to the completion of PIAs, that office should be respected and seen as a legitimate "internal privacy advocate", by virtue of its history, organisational independence and reputation of senior personnel.

For those few officials within the federal bureaucracy who are steadfastly attempting to advance the privacy argument, PIAs do provide a valuable tool. As Ari Schwartz, Deputy Director of the Center for Democracy and Technology has commented, they do "motivate people who want to do the right thing, to do the right thing."[44] However, most

[40] Quoted in Jason Miller, "Serious about Privacy," ref 38.
[41] US Governmental Accountability Office, *Homeland Security: DHS Privacy Office has Made Progress but faces Continuing Challenges*, Statement by Linda Koontz, Director Information Management Issues, GAO-07 1024T at: http://www.gao.gov/new.items/d071024t.pdf
[42] Kenneth A Bamberger and Deidre Mulligan, "Privacy Decision-Making in Administrative Agencies," *Chicago Law Journal* (forthcoming).
[43] See David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).
[44] Interview, Ari Schwartz, August 10, 2007

federal agencies do not have privacy offices with a statutory basis and with adequate staff. In 1998, the Clinton Administration required all agencies to designate a senior official within the agency to assume primary responsibility for privacy policy and to review *Privacy Act* compliance within each agency. In 1999, the Administration appointed a Chief Privacy Counselor for the Administration within the OMB. In 2001, despite urging from privacy advocates, the Bush Administration did not hire a new Chief Privacy Counselor in the OMB. American privacy advocates continue to press, therefore, for effective privacy officer functions in every federal agency with: (1) a statutory basis; (2) adequate staff; and (3) involvement in senior-level policy deliberations.[45] These conditions are generally regarded as necessary for the advancement of privacy protection policy generally, as well as for the conduct of PIAs in particular.

Transparency of output, but a lack of external consultation during the PIA process

The presumption of publicity embedded within the Electronic Government Act helps to render transparent some personal information systems that would otherwise be clouded in secrecy. For those outsiders with the time, energy and commitment, they do serve as one, albeit imperfect, instrument of accountability. The more thorough PIAs provide important raw material for privacy professionals within government, for Congress and for privacy advocates to ask the right questions about the collection, use and disclosure of personal information.

As there is no requirement under the E-Government legislation for outside consultation, however, then procedures have naturally developed to emphasise the importance of PIAs as "pre-decisional" instruments for the benefit of internal review and analysis. And while there seems to be a general consensus among American privacy advocates that it is, on balance, better to have PIAs conducted and published than not, there is also a series of question marks about whether the internal procedures really do result in significant changes to a programme in response to internal arguments about privacy risks.

There have been occasions when the delays of publication of PIAs have been criticised. In November 2006, the DHS provided additional notice in the *Federal Register* of the Automated Targeting System (ATS), the process of security ratings of American citizens of millions of travelers, based on the same risk-assessment methodologies designed for the screening of cargo coming into the United States. DHS announced that the programme would go into effect on December 4, 2006. In its comments, the American Civil Liberties Union complained that: "the program's Privacy Impact Assessment (PIA) was not made available to the public until November 27 – only one week before the program is slated to go into effect. Given that the PIA represents the most comprehensive explanation of the system provided to the public, that is simply not a reasonable amount of time. It does not allow respondents to adequately analyze the privacy impact statement and its implications, formulate comments articulating that analysis clearly, and submit them with time for Department of Homeland Security to properly consider them before the program becomes effective."[46] Similar criticisms were levied against the PIA process for the US Visit programme, a "forthright and clear analysis of the privacy issues involved" according to Jim Dempsey of CDT, but one that

[45] Statement by Jim Dempsey of Center for Democracy and Technology, House Committee on the Judiciary Subcommittee on Commercial and Administrative Law, February 10, 2004 at: http://www.cdt.org/testimony/20040210dempsey.shtml#f2#f2.
[46] http://www.aclu.org/privacy/gen/27593leg20061201.html.

would have been "far more meaningful if it had been issued before the program was actually being implemented."[47]

While public input post-PIA and post-programme design can result in privacy-enhancing changes, it also takes concerted effort on the part of external privacy advocates, and the programme costs can often be greater. Where programmes have undergone significant change, in some part as a result of external criticism, the PIAs do provide interesting comparative reference points. The programme called "Secure Flight" is a case in point. First announced in 2004 as a successor to the Computer Assisted Passenger Profiling System (CAPPS), Secure Flight was designed as a passenger pre-screening tool to authenticate information on air travelers with records stored in government databases, and with data purchased from unspecified commercial data aggregators. There was an enormous amount of criticism, not only from the privacy advocates, but also from a series of reports within the General Accounting Office (GAO). The programme was reconsidered and reintroduced in August 2007, together with a new PIA.[48] As with other controversial surveillance systems associated with the Bush Administration's "War on Terror,"[49] these programmes carry high political stakes and have been the product of an extraordinary amount of attention from media and civil liberties groups. If programmes are altered, it is generally impossible to know whether that is in response to the internal PIA process, or to the wider publicity and criticism.

System of Records

The PIA process in the United States is generally internal to a particular agency. It is tied to a model of privacy oversight (which dates from the 1974 *Privacy Act*) through the analysis of discrete systems of records for which defined agency personnel have responsibility. This issue speaks to a larger structural problem with the enforcement of privacy protection rules in all advanced industrial states. How can responsibility for the processing of personal information be properly assigned when the larger technological and informational environment encourages a free flow of personal information across instutitonal and technological boundaries? Two challenges can be mentioned briefly.

First, there is little guidance as to how PIAs might be conducted wtihin an inter-agency framework. For example, there seems to be lack of clarity between the relationship between PIAs and the process of review when computer matching between different systems of records occurs. The comparison of different files to identify individuals who might be illegally claiming benefits, for example, is regulated under the 1988 *Computer Matching and Privacy Protection Act*, and the Data Integrity Boards established under this legislation to approve these matching programmes.

Second, there is a larger and more controversial question about the increasing reliance on commercial databases to achieve public policy goals, and whether or not reliance on existing private sector systems constitutes a "collection" of personal information under the *Privacy Act*.[50] At one level, the issue is a legal one. At another level, it must be noted that the institution of PIA methodology in the US has taken place within the context of a wider debate about the increasing tendency of the US government to rely on commercial

[47] Jim Dempsey, Statement, February 10, 2004.
[48] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.
[49] Programmes such as Secure Flight, the Automated Targeting System, the U.S. Visit Program and the Trusted Traveler program.
[50] Jim Dempsey, Statement, February 10, 2004.

databases for a range of policy goals, and the consequent concerns about wider trends towards ever more extensive and intrusive methods of surveillance.[51]

Conclusion

The statutory mandate for the conduct of PIAs in the US produces some peculiar conditions and incentives which cannot translate to the UK context. Furthermore, the absence of the equivalent institution to the ICO, means that the larger questions about external review of PIAs by a privacy oversight agency cannot really be addressed in the US context. However, this brief review underlines the importance of publication, and it does suggest the need for procedures for external stakeholder consultation, at least for PIAs on major projects. Most especially, the American experience emphasises the significance of internal and institutionalised privacy expertise which can use the PIA methodology to inject privacy reasoning into internal agency deliberations at the earliest stages of decision-making and for the entire life-cycle of the project. At the end of the day, however, PIAs are only as good as the standard to which they are being conducted. In the US, that standard is principally the *Privacy Act* of 1974, a statute that for many years has been regarded as outdated, permissive of too many exemptions and "routine uses," unable to provide meaningful remedies and redress for individual citizens, and insufficiently sensitive to the realities of contemporary data processing.[52]

Research

The following individuals were interviewed:

Department of Homeland Security (practitioner):

- Rebecca Richards, Director of Privacy Compliance

Center for Democracy and Technology (privacy advocate):

- Ari Schwartz, Deputy Director

In addition, a number of primary and secondary sources were consulted, as indicated in footnotes.

[51] See for example the arguments in Daniel Solove, *The Digital Person* (New York: NYU Press, 2005), pp. 168-75.
[52] Among others, see Solove, *The Digital Person,* pp. 136-8; Robert Gellman, "Does Privacy Law Work? in Agre and Rotenberg eds. *Technology and Privacy,* pp. 193-218; David H. Flaherty, *Protecting Privacy in Surveillance Societies,* pp. 359-61.