U.S. ACCOUNTABILITY AND OVERSIGHT FOR PRIVACY INFORMATION

I. INTRODUCTION

The Constitution of the United States, under a doctrine known as separation of powers, divides authority among three branches of government – the legislative, executive and judicial. The legislative branch makes law, the executive branch executes it and the judicial branch interprets it. Members of all three branches are appointed or elected for specified terms. In addition, the powers of one branch may be challenged by another branch under a system of checks and balances.

Following is a list of the primary checks that each branch may exercise on the other branches:

A. Executive Branch

1. Checks on the Legislature
    - President may veto legislation; however, see below on the power of the legislature to override a President's veto
    - Vice President is President of the Senate
    - President is Commander in Chief of the military
    - President may make recess appointments of senior Governmental Officials who would otherwise require confirmation of the Senate; however, these recess appointments are of limited duration to ensure that the Senate's power is not abrogated
    - President may call one or both houses of Congress into session in the event of an emergency
    - President may force adjournment when both houses cannot agree on adjournment
2. Checks on the Judiciary
    - President has the power to appoint judges
    - Pardon power
3. Checks on the Executive
    - Vice President and Cabinet can vote that the President is unable to discharge his duties

B. Legislative Branch

- Checks on the Executive
    - Impeachment power (House)
    - Trial of impeachments (Senate)
    - Selection of the President (House) and Vice President (Senate) in the case of no majority of electoral votes
    - May override Presidential vetoes
    - Senate approves Executive Departmental appointments
    - Senate grants advice and consent to ratification of treaties and confirms appointment of ambassadors
    - Approval of replacement Vice President

    - Power to enact taxes and allocate funds
    - President must, from time-to-time, deliver a State of the Union address
    - Power to audit through Government Accountability Office
- Checks on the Judiciary
    - Senate approves federal judges nominated by the President
    - Impeachment power (House)
    - Trial of impeachments (Senate)
    - Power to initiate amendments to the U.S. Constitution. Must be approved by 2/3 of each house of Congress
    - Power to establish courts inferior to the Supreme Court
    - Power to establish jurisdiction of courts
    - Power to alter the size of the Supreme Court
- Checks on the Legislature – because it is bicameral (House and Senate), the Legislative branch has a degree of self-checking
    - Bills must be passed by both houses of Congress
    - House must originate revenue bills
    - Neither house may adjourn for more than three days without the consent of the other house
    - All journals are to be published

C. Judicial Branch

- Checks on the Legislature
    - Judicial review
    - Seats are held on good behavior
    - Compensation cannot be diminished
- Checks on the Executive
    - Judicial review
    - Chief Justice sits as President of the Senate during presidential impeachment

Set forth below are the core U.S. Government oversight mechanisms that are utilized in this system of checks and balances. Today, the many traditional organizational checks on authority merge with newer, specialized authorities to ensure all governmental authorities comply with U.S. law and policy regarding the protection of individual privacy.

II. ACCOUNTABILITY AND OVERSIGHT

This section summarizes the U.S. governmental oversight framework with emphasis on law enforcement and home affairs agencies. Oversight is achieved through powers exercised by Congress, the executive branch and the judiciary as set out in the U.S. Constitution. Within each of these branches exists a variety of oversight bodies that independently review, assess and report on the actions of federal agencies, including the failures, shortcomings and recommended corrective actions. Each oversight body also has procedures and measures to compel an agency to change policies or systems that are inconsistent with law, policy or otherwise threaten fundamental rights.

The core privacy authorities for U.S. Government use of personally identifiable information can be found in the U.S. Privacy Act of 1974, the Freedom of Information Act (FOIA) and the E-Government Act of 2002, which are also supported by a framework of regulations,[1] Executive Orders [2] and other policies.[3] Other U.S. laws such as the Federal Information Security Act (FISMA) provide for the security of sensitive information that includes protections for personally identifiable information.

A. Executive Branch

1. OMB

The executive branch implements privacy laws through notices, regulations,[4] Executive Orders and Directives. The Office of Management and Budget (OMB), an office within the White House that reports directly to the President, provides leadership to all executive agencies by issuing Directives and Memoranda on how best to implement privacy laws as well as other directives.[5]

2. Agencies

a. Chief Privacy Officers

In 2005, through OMB Memorandum, OMB required that all federal agencies appoint a senior agency official to assume primary responsibility for privacy policy. This official, usually titled Chief Privacy Officer (CPO), enforces privacy policy and provides guidance tailored to the particular agency, monitors compliance with applicable laws and policies and supports requests for information and redress from the public.

Desiring to give the Chief Privacy Officer more authority, in 2003, Congress created the first statutorily mandated CPO with the advent of the Department of Homeland Security.[6] The DHS CPO's statutory duties include: 1) assure that new technologies do not erode privacy; 2) assure that personal information in Privacy Act Systems of Records is handled in compliance with the FIPs as set out in the Privacy Act; 3) evaluate new legislation on personal information; 4) report to Congress; and 5) coordinate with the DHS Civil Rights and Civil Liberties Office.

---

[1] Regulations are rules and administrative codes issued by governmental agencies at all levels: municipal, county, state and federal. Although they are not laws, regulations have the force of law, since they are adopted under authority granted by statutes, and often include penalties for violations.

2 Executive Orders are a President's or Governor's declaration that has the force of law, usually based on existing statutory powers, and requiring no action by the Congress or state legislature.

3 A policy is a plan of action to guide decisions and actions.

[4] An Executive agency that intends to adopt a rule must give public notice of its intention in the *Federal Register*. The published notice, called a Notice of Proposed Rulemaking (or "NPRM"), typically requests public comment on a proposed rule, and provides notice of any public meetings where a proposed rule will be discussed. The public comments are considered by the issuing government agency, and the text of a final rule is published in the *Federal Register*.

[5] For a complete set of privacy guidance directives issued by OMB, see: http://www.whitehouse.gov/omb/privacy/index.html.

[6] Homeland Security Act of 2003, section 222(f).

Believing that the DHS CPO was a successful oversight mechanism, Congress further mandated the appointment of a Chief Privacy Officer at the Department of Justice (DOJ) and also separately required that other Executive Branch Departments appoint CPO's. Even though the CPO's position is integral to the agency, e.g., helping ensure that privacy considerations are integrated into all programs, the CPO also maintains independence from the Department, for example, by a requirement to prepare an annual report to Congress on departmental activities that affect privacy including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.

When Congress reformed the intelligence apparatus in the U.S. Government through the Intelligence Reform and Prevention Act (IRTPA) of 2004, giving intelligence agencies more powers to fight terrorism, it also created a Civil Liberties Protection Officer in the Office of the Director of National Intelligence and mandated creation of the Privacy and Civil Liberties Oversight Board.[7] Both of these offices act as oversight on the increased powers given to the intelligence community in the IRPTA. The Board consists of five members appointed by the President with the Chairman and Vice Chairman confirmed by the Senate. The Board advises the President with respect to privacy and civil liberties in the implementation of all laws, regulations and executive branch policies related to efforts to protect against terrorism. In addition, the Board is specifically charged with reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed. The Board provides advice and recommendations to the President and executive branch department and agency heads, as appropriate, and additionally makes an annual report to Congress.

b. Rule Making and Funding

Privacy laws ensure transparency in the personally identifiable information that federal agencies collect from the public. The Privacy Act of 1974 requires that the individual be provided notice of the agency's use, dissemination and maintenance of the personally identifiable information it collects. There are several administrative processes required by these laws that allow the public an opportunity to receive and consider notice of an agency's collection or use of personally identifiable information.

For instance, the Privacy Act requires agencies to publish in the Federal Register Systems of Records Notices (SORNs) that specify how an agency maintains personally identifiable information, its purposes for collection and any allowances for the use and disclosure of a record without the prior consent of the individual. Agencies must also notify the public of how an individual may seek access, correction and redress for information contained about the individual in the system of record. The SORN must be submitted to OMB and to Congress for 40 days of review, concurrent with the publication of the SORN in the Federal Register.

Additionally, the Privacy Act allows for the exemption of certain records, such as individual law enforcement records, from certain requirements of the Privacy Act. In order to request an exemption for eligible records, an agency must publish in the Federal Register a Notice of Proposed Rule Making (NPRM) in which the agency explains in detail what particular

[7] http://www.privacyboard.gov/

exemptions are being requested and the specific reasons why. Public comments received on a NPRM must be reviewed by the agency and the agency must respond to these comments in a subsequent Federal Register notice before issuing the final rule. The rulemaking process is used to allow individuals and organizations to comment on such collections before an agency may issue these rules and notices as final.

Under the statutes that created the Chief Privacy Officer and Civil Liberties Protection Officer in the Office of the Director of National Intelligence, each officer is responsible for reviewing and approving all Privacy Impact Assessments (PIAs). A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. PIAs are posted on a federal agency's website[8] and published in the Federal Register.[9] Indeed, PIAs must be published in order to receive funding by OMB.[10]

c. Redress and Inquiry through the Administrative Process

The FOIA provides any person an administrative process to seek access to information about them.[11] Closely associated with this is the Privacy Act that requires agencies to have an administrative process to allow U.S. persons to seek access and amendment to records about them, subject to certain exemptions. While the Privacy Act does not grant rights of amendment to non-U.S. persons,[12] some agencies have established an administrative process apart from the procedures provided by the Privacy Act that allows non-U.S. persons the opportunity for redress of information concerning them. For example, the DHS Traveler Redress Inquiry Program (TRIP) allows any individual—regardless of nationality—to seek redress for the records maintained by DHS components responsible for transportation and border security.[13]

d. Policy Commitments

While not binding, privacy policy commitments made by the head of an agency are carried out and enforced by senior agency officials. For instance, in the case of DHS, Secretary Chertoff has urged the Privacy Office to apply strong privacy protections for all persons included in DHS systems, regardless of citizenship.

> *If we want to protect the privacy of our own citizens, we are going to have to be willing to protect the privacy of our international partners and their citizens. And that means we have to protect shared information and continue to demonstrate a level of trust ... I trust*

---

[8] See for example, www.dhs.gov/privacy
[9] The Federal Register is also available on the world wide web. See http://www.gpoaccess.gov/fr/index.html
[10] See OMB M-03-22 Memorandum, http://www.whitehouse.gov/omb/memoranda/m03-22.html
[11] For example, in 2005 the Department of Justice processed 51,435 FOIA requests. That same year, the Department of Homeland Security processed 126,126 requests. Of those, DHS received 37 FOIA requests from 17 countries.
[12] For ease of reference, this article will refer to those covered by the Privacy Act as ''U.S. persons'' and those not covered as ''non-U.S. persons.'' The Privacy Act applies to ''a citizen of the United States or an alien lawfully admitted for permanent residence.'' 552a(a)(2).
[13] See DHS Privacy Office website at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf

> *that the Privacy Office will be equally vigorous in insuring that American data is protected in the EU to the same or a higher degree.*[14]

This was followed by a Department-wide policy issued by the DHS CPO to afford privacy protections for non-U.S. persons in DHS systems of records.[15]

e. Inspectors General

Every large U.S. government agency, including DHS and DOJ, has an Inspector General (IG). Inspectors General are authorized by law to conduct independent investigations, audits, inspections and special reviews of individual actions and programs to detect and deter waste, fraud, abuse and misconduct. In addition to required bi-annual reports to Congress, Congress may require that the IG provide specialized reports or the IG may independently determine to initiate an investigation. Such investigations may include privacy related issues. For example, the Department of Justice Inspector General recently issued a report to Congress on the FBI's use of National Security Letters.[16] The Department of Homeland Security Inspector General concluded an investigation into DHS's handling of Personally Identifiable Information.[17] The process is transparent with IG reports publicly available. Inspectors General often work with the Privacy Offices at DHS, DOJ and DNI to assist with their oversight functions.

f. Administrator of General Services or the Archivist

The Archivist, appointed by the President without regard to political affiliation and confirmed by the Senate, is authorized by law to "inspect the records or the records management practices and programs of any Federal agency" for the purpose of making recommendations for improving records management practices and programs. This may extend to an examination of privacy records. Agencies are also required to obtain approval of the Archivist for retention schedules and follow its guidance for deletion.

B. Congress

1. The Government Accountability Office (GAO)

The GAO, which is independent and nonpartisan, is Congress' investigative arm. At Congressional request, the GAO investigates audits and evaluates executive branch agencies and the programs and expenditures of the Federal government. The GAO is created by statute, which specifically defines its powers to conduct reviews and investigations and issue legal opinions. When GAO reports its findings to Congress and the heads of executive departments and agencies, it recommends actions. It has issued numerous reports analyzing agencies' handling of personal information specifically addressing law enforcement and national security.[18] For

---

[14] DHS Secretary Michael Chertoff, prepared remarks delivered to the DHS Privacy Advisory Committee, December 6, 2005.
[15] Policy statement can be found at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[16] http://www.usdoj.gov/oig/
[17] http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_07-24_Jan07.pdf
18 For GAO reports on law enforcement and homeland security information systems as well as numerous other topics, see http://www.gao.gov/

example, the GAO conducted extensive investigations and reported on privacy protections and compliance in a DHS aviation security system called Secure Flight[19]. Its final recommendations to DHS included taking several actions to manage risks associated with Secure Flight's development, such as finalizing privacy and redress requirements. In early 2007, the GAO completed reviews and reports on health information technology[20] and data privacy and improvements to FOIA.[21]

2. Congressional Committees

Congress is also within its Constitutional powers to conduct direct oversight on executive branch activities through its committees. Congress could issue reports and withhold funding based on negative findings in an investigation of an agency's handling of personal information.

The frequency and level of hearings and the level of detail they may cover can be extensive. For example, in 2006, DHS officials testified at 206 hearings, conducted approximately 2,242 congressional briefings and received more than 2,000 post Hearing Questions for the Record.

C. Judiciary

Under the FOIA, any person may challenge an agency's response to his or her FOIA request in federal court. Access to the court system is permitted regardless of citizenship or resident status. Agencies must comply with court orders regarding access to records.

The Privacy Act provides for four separate and distinct civil causes of action—two of which are injunctive (amendment and access) and two of which provide for monetary damages (accuracy lawsuits and lawsuits for other damages).[22] The limitation, however, is that non-U.S. persons are not granted standing in the courts to pursue claims under the Privacy Act. Non-U.S. persons may seek amendment of their records through administrative programs established outside the procedures afforded by the Privacy Act like the DHS Traveler Redress and Inquiry Program, however.

D. The Public Privacy Community

The executive branch, Congress and the judiciary are the formal actors under the Constitution. There are also other less formal but still influential oversight mechanisms. The U.S. enjoys a large and active advocacy community consisting of non-governmental organizations dedicated to privacy and related civil liberties. These groups are accepted as part of the democratic process and serve as vigorous public watchdogs. Agencies frequently seek their input through written and oral consultations. During the notice and comment period of privacy regulations, comments from the advocacy community are often the most informed.

---

[19] http://www.gao.gov/new.items/d05356.pdf
[20] http://www.gao.gov/new.items/d07400t.pdf
[21] http://www.gao.gov/new.items/d07491t.pdf
[22] See 5 U.S.C. 552a(g).

III. RECOGNITION OF U.S. OVERSIGHT INTERNATIONALLY

The U.S. has a number of agreements and arrangements in the law enforcement, public and national security area where U.S. privacy oversight and accountability has been recognized internationally. As a Member of the European Parliament and Rapporteur of the Committee on Civil Liberties, Justice and Home Affairs, Sophie In't Veld, recently commented, "[t]he U.S. has much stricter privacy rules than Europe, and they are much better at democratic oversight and self-criticism."[23]

In the past five years, European Union institutions and member states have repeatedly demonstrated confidence in the United States' ability to protect personally identifiable information exchanged for law enforcement and public safety purposes. This respect for the U.S.' handling of personal data and respect for its mechanisms for maintaining accountability has been demonstrated through execution of several binding international agreements. In December 2001, the United States and Europol signed a cooperation agreement, and in December 2002 a supplemental agreement for the sharing of personally identifiable information. In November 2006, the U.S. and Eurojust concluded a cooperation agreement for the sharing of personally identifiable information. Article 12 of the 2002 Europol supplemental agreement provides that the United States shall conduct oversight of its implementation in accordance with applicable law and procedures, utilizing administrative, judicial or supervisory bodies that ensure an appropriate level of independence. Article 19 of the 2006 Eurojust agreement contains a similarly-worded provision. The Europol and Eurojust Agreements were approved by those institutions' data privacy supervisory authorities, and in effect serve as formal determinations that conditions for sharing information with the United States have been met.

In addition, in June 2003, the United States and the European Union concluded agreements on Mutual Legal Assistance and Extradition. Subsequently, all 25 member states (before the January 2007 enlargement) concluded bilateral instruments with the United States implementing these agreements. Among the provisions in the Mutual Legal Assistance agreement is an article governing the use of personal data in the context of criminal investigations and prosecutions, related administrative proceedings and for preventing imminent and serious threats to public security. This provision, drawn from the U.S.-Germany Mutual Legal Assistance Treaty, both ensures prosecutors the flexibility they need and protects personal data in line with the requirements of European legislation.

In reviewing the U.S.-EU PNR Agreement and Undertakings, the EU Advocate General in the PNR cases observed that, "The Chief Privacy Officer is not a judicial authority. However...the Officer is an administrative authority with some degree of independence from the Department of Homeland Security."[24] The Advocate General went on to find that allowing "airline passengers to lodge a complaint with the Chief Privacy Officer and the availability to them of a judicial remedy under the FOIA constitute significant safeguards with regard to their right to respect for their private life."[25]

---

[23] http://www.neurope.eu/view_news.php?id=71636
[24] Opinion of the EU Advocate General, Cases C-317/04 and C-318/04, November 22, 2005, paragraph 252.
[25] Id at 253.

Implicit in this is the EU acceptance that the U.S. framework provides acceptable powers of accountability and oversight over personally identifiable information. Since the U.S. and EU have different systems of government, this language allowed for mutual recognition of our varying systems.

Outside of the EU, the U.S. and Canada negotiated an agreement to share asylum data. In this case, both systematic and case-by-case sharing of asylum information between Canada and the U.S. is allowed under a formal arrangement known as the Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims (the "Annex"), which falls under an umbrella agreement, the Statement of Mutual Understanding on Information Sharing between Canada and the United States. Before signing the Annex, U.S. and Canadian governments carefully considered each other's confidentiality and privacy rules and practices to gain assurance that shared information would be protected appropriately. The privacy and confidentiality rules of each country also required that certain steps be taken at high-levels of the government before implementing the information-sharing arrangement. The Canadian government performed a Privacy Impact Assessment in order to demonstrate that the sharing of asylum information under the Annex would not unduly affect the asylum applicants' privacy rights. The Privacy Impact Assessment was reviewed and approved by Canada's Privacy Commissioner.

Additionally, the Department of State and DHS entered into personal information sharing commitments with Australia and New Zealand to protect privacy of individuals in an MOU[26] to share lost and stolen passport information. By signing the MOU, each party explicitly recognized the other party's high level of oversight and enforcement of data privacy provisions related to the information being exchanged.[27]

Finally, while outside the scope of traditional criminal law enforcement and home affairs, it is worth nothing that U.S. independent agencies share confidential personally identifiable information with foreign law enforcers for purposes of investigating or pursuing fraud, deception, spam, spyware and other commercial violations.[28] Such investigations can later be referred to the Attorney General for prosecution. These exchanges are further international recognition of the effective oversight and accountability of U.S. agencies over personally identifiable information.

IV. CONCLUSION

Viewed as a whole, effective oversight and accountability in the U.S. is achieved through a combination of Congress, the executive branch and the judiciary exercising their Constitutional authorities.

---

[26] http://www.apec.org/apec/documents_reports/informal_experts_group_business_mobility/2006.html

[27] For a discussion of the privacy of non-U.S. persons in the context of international agreements, see Kropf, The Privacy of Foreign Nationals, BNA Privacy and Security Law Report, Vol. 3, No. 46. at 1306 (November 15, 2004).

[28] For example, the Federal Trade Commission (FTC) has entered into bilateral cooperation agreements with agencies in Australia, Canada, Ireland, Mexico and the United Kingdom and executed memoranda of understanding on spam enforcement with agencies in Australia, the United Kingdom and Spain.