Privacy Decisionmaking in Administrative Agencies

Kenneth A. Bamberger† *& Deirdre K. Mulligan*††

INTRODUCTION[1]

Administrative agencies increasingly rely on technology to promote the substantive goals they are charged to pursue. The Department of Health and Human Services has prioritized digitized personal health data as a means for improving patient safety and reducing bureaucratic costs.[2] The DOJ hosts electronic databases that pool information between agencies to facilitate national law enforcement in ways previously unimaginable.[3] The Departments of Defense and Education mine digital information to effect goals as diverse as human resources management; service improvement; fraud, waste, and abuse control; and detection of terrorist activity.[4]

The use of technology to achieve the principal purposes set forth in agency enabling statutes—health, security, or education, for example—has significant consequences for other public goals. Specifically, the digital collection of personally identifiable information renders

---

† Assistant Professor of Law, UC Berkeley School of Law.

†† Clinical Professor of Law; Director, Samuelson Law, Technology & Public Policy Clinic; Director, Clinical Program, UC Berkeley School of Law. Much appreciation to Colin Bennett, Malcolm Crompton, Peter Cullen, Lauren Edelman, Robert Gellman, Chris Hoofnagle, Robert Kagan, Jennifer King, Anne Joseph O'Connell, Fred B. Schneider, Ari Schwartz, Paul Schwartz, and the participants at The University of Chicago Law School's Surveillance Symposium for insight, comment, and discussion; Nuala O'Connor Kelly and Peter Swire for consenting to be interviewed about their experience in privacy leadership roles within the United States government; Sara Terheggen, Marta Porwit Czajkowska, Rebecca Henshaw, and Andrew McDiarmid for their able research.

1 This paper is an extension of the authors' national study of corporate Chief Privacy Officers, *Catalyzing Privacy: Corporate Privacy Practices under Fragmented Law* (unpublished manuscript, 2007), funded by the Rose Foundation for Communities and the Environment and by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422).

2 See Department of Health and Human Services, *Harnessing Information Technology to Improve Health Care* 1 (May 6, 2004), online at http://www.providersedge.com/ehdocs/ehr_articles/Harnessing_Information_Technology_to_Improve_Health_Care.pdf (visited Jan 12, 2008) (providing an overview of opportunities to improve health care through technology).

3 See, for example, FBI, *IAFIS: Integrated Automated Fingerprint Identification System*, online at http://www.fbi.gov/hq/cjisd/iafis.htm (visited Jan 12, 2008) (detailing the technology behind a national fingerprint and criminal history system maintained by the FBI).

4 See GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548, 2–3 (May 2004), online at http://www.gao.gov/new.items/d04548.pdf (visited Jan 12, 2008) (reporting on operational and planned data mining systems and activities in federal agencies).

that data subject to the immense search and aggregation powers of technology systems, increases the capacity for repurposing and reuse, and provides increasingly attractive targets to hackers bent on misuse. These phenomena raise serious concerns about a surveillance capacity that can erode personal privacy.

The digitization of administration, then, raises the question of how to ensure that decisions about the use of technology in public management reflect not only the direct mandates with which particular agencies and administrators are specifically charged, but also political and social commitments to universal privacy concerns.

Recognizing that the "rapid evolution of information technology has raised questions about whether personal information is adequately protected,"[5] Congress, in the E-Government Act of 2002,[6] required administrative agencies to conduct privacy impact assessments (PIAs) when developing or procuring information technology systems that include personally identifiable information.[7] The Office of Management and Budget (OMB) guidance promulgated pursuant to the statute mandates that PIAs include a risk assessment that specifically identifies and evaluates potential threats to individual privacy, discusses alternatives, identifies appropriate risk mitigation measures, and articulates the rationale for the final design choice.[8] OMB Director Joshua Bolten issued requirements of considerable institutional breadth—the process would influence decisions not only across agencies, regardless of primary mission, but also in the executive branch and by federal contractors.[9] Further, the requirement applies both to new technology systems and to "new privacy risks" created when changing existing systems.

Despite this new privacy requirement, adherence to privacy mandates across agencies—and even between programs within a single agency—is highly inconsistent. In this paper, we engage in an initial exploration into the explanation for the PIA requirement's uneven success in making agencies incorporate privacy concerns into technology decisions.

---

5 Great Falls Historic District Study Act of 2001, S Rep No 107-74, 107th Cong, 2d Sess 8 (2002).

6 Pub L No 107-347, 116 Stat 2899.

7 44 USC § 3501 note (2000 & Supp 2002) (requiring agencies to conduct a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form").

8 See OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept 26, 2003), online at http://www.whitehouse.gov/omb/memoranda/m03-22.html (visited Jan 12, 2008).

9 See id.

The record of inconsistency suggests the insufficiency of decision process requirements alone to ensure the uniform inclusion of privacy objectives in policymaking. This suggestion seems especially salient given that privacy is a secondary concern for agencies and frequently in tension with their primary mandates.

It also underscores the contextual contingency of political oversight as a means for ensuring uniform control of delegated discretion. These accountability shortcomings, we argue, are particularly relevant in light of two characteristics of the privacy context: the political sensitivity inherent in the public promotion of privacy and the enhanced barriers to transparency in decisions about technology. As to the former, privacy remains contested when compared to the interests against which it is frequently juxtaposed—physical security and administrative efficiency. This can create strong disincentives for politically accountable actors to promote its protection in specific policy choices.[10] As to the latter, discussions about choices between information systems are frequently cloaked in either the inaccessible idiom of technology or the disinterested language of bureaucracy, both of which may create practical barriers to effective advocacy and oversight.

Having suggested limits to traditional means of external oversight in the privacy context, we explore what factors might, by contrast, promote the consideration of privacy. To that end, we examine the implementation of the PIA requirement by two different federal agencies considering the adoption of a single technology: radio frequency identification (RFID), which allows a data chip—one that can be accessed remotely by wireless technology—to be attached to or inserted into a product, animal, or person.

The first agency, the Department of State (DOS), proposed a rule incorporating RFID technology into US passports. Its one and one-half page "e-Passport" PIA, consisting of seven paragraphs, failed to discuss the technical aspects of the program, alternative technologies, risks, or their mitigation. The program was ultimately adopted with significant modifications amidst criticism as to its security vulnerabilities and privacy risks.

---

[10] The unwillingness of Congress to require the Administration to comply with the requirements of the Foreign Intelligence Surveillance Act (FISA), Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USCA § 1801 et seq (2007), and its likely decision to retrospectively immunize the telecommunications providers who aided the government in its illegal surveillance program, exemplify this problem and highlight the particular strain domestic terrorism places on privacy oversight by politicians.

By contrast, the PIAs produced by the Department of Homeland Security (DHS) during its adoption of the same technology[11] in the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program contained forty-eight single-spaced pages. The assessment detailed the system architecture, privacy threats and mitigation methods, an explanation of their design choice, and a plan for implementing any necessary additional privacy and security measures on an ongoing basis. The program, as proposed and adopted, reflected these assessments.[12]

Comparing our two cases suggests the importance of internal agency structure, culture, personnel, and professional expertise as important mechanisms for ensuring bureaucratic accountability to the secondary privacy mandate imposed by Congress. Building on literature identifying and documenting factors that contribute to successful data protection efforts, our case study explores the relationship between independence, agency culture, expertise, alternative forms of external oversight, interest group engagement, and the management of privacy commitments within federal agencies.

---

11 The particular standards used varied (e-Passport ISO 14443, US-VISIT) but the basic technology is the same.

12 Section 7208(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 required US-VISIT to collect biometric exit data from all individuals who are required to provide biometric entry data. Pub L No 108-458, 118 Stat 3638, 3819, codified at 8 USC § 1365b(d) (Supp 2004). In response, DHS proposed Increment 2C, which intended to use passive RFID tags embedded in the I-94 arrival/departure form to track entry and exit of foreign visitors at land border Point Of Entry crossings. DHS, *Notice of Privacy Act System of Records*, 70 Fed Reg 38699, 38699–700 (2005). The embedded tag stored no personally identifiable data; instead, each tag contained a unique identifier that was linked to a traveler's information in the US-VISIT database. Id at 38700. DHS conducted a feasibility study (final report issued January 21, 2005) and commenced testing of the proposed system. See GAO, *Homeland Security: Prospects for Biometric US-VISIT Exit Capability Remain Unclear*, GAO-07-1044T, 10 (June 28, 2007), online at http://homeland.house.gov/SiteDocuments/20070628154223-99040.pdf (visited Jan 12, 2008) (pointing to reliability problems in tests of the proposed system at five points of entry); DHS, *US-VISIT Increment 2C RFID Feasibility Study: Final Report* (Jan 21, 2005), online at http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDfeasibility_redacted-051106.pdf (visited Jan 12, 2008) (proposing recommendations based upon the feasibility study). A GAO report issued in January 2007 noted that in addition to technical deficiencies with the proposed system, "the technology that had been tested cannot meet a key goal of US-VISIT—ensuring that visitors who enter the country are the same ones who leave." GAO, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-378T, 21 (Jan 2007), online at http://www.gao.gov/new.items/d07378t.pdf (visited Jan 12, 2008).

DHS Secretary Michael Chertoff announced in February 2007 while testifying before the House Homeland Security Committee that DHS was abandoning the program due to its inability to meet its primary objective of identifying the flow of I-94 carriers across borders. See *Chertoff: RFID Program to Be Abandoned*, UPI (February 9, 2007). The authors believe the intense examination of the program's objective, performance, and risks that led to its abandonment was greatly facilitated by the PIA process and the ongoing examination and attention to the privacy and security issues posed by the program by the Data Privacy and Integrity Advisory Committee, Congress, and the public.

We hope that this early analysis proves interesting for debates in both public administration and privacy protection. In particular, we consider ways in which these early and limited experiences with PIAs might speak to the debate on the efficacy of external controls on bureaucracy, and to the less-developed literature seeking to open the "black box" of administrative decisionmaking by exploring the structural, organizational, and human factors at work within agencies. As to privacy, we believe these early experiences provide insight into preconditions necessary to advance privacy commitments through administrative structures in the face of social and bureaucratic pressures to manage risk by acquiring information about individuals. Finally, we suggest implications for specific proposals for policy reform intended to promote agency accountability to privacy goals.

I. PRIVACY MANDATES AND INCONSISTENT IMPLEMENTATION

A. The PIA Mandate

In the face of increased digitization of information, Congress included the PIA requirement in the 2002 E-Government Act. The PIA provisions mandated, in the words of the bill's Senate report, that agencies publicly "explain"—by means of a PIA—how they "take[ ] into account privacy considerations when purchasing and creating new information systems, and when initiating collections of information."[13] "[T]he greater personalization of government services," the report continued, "need not impinge on personal privacy, if the federal government takes steps to address privacy concerns when first designing systems."[14]

The PIA provisions augmented the approach of the Privacy Act of 1974,[15] which relies principally on notice as the procedural mechanism for safeguarding personally identifiable records.[16] That law prohibits agencies, in most instances, from disclosing personal records beyond the "routine use" for which they were collected without written consent from the individual to whom the records pertained.[17] Implementation of its recordkeeping and safeguarding requirements was assigned largely to midlevel agency employees responsible for other

---

13 S Rep No 107-74 at 28–29 (cited in note 5).

14 Id at 28 (addressing one of two major concerns in privacy policy, the other being clarity of privacy notices).

15 Pub L No 93-579, 88 Stat 1896, codified as amended at 5 USC § 552a (2000 & Supp 2004).

16 Specifically, the Act governs records contained in a "system of records," which includes "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 USC § 552a(a)(5).

17 See 5 USC § 552a(b).

tasks besides the privacy function.[18] Furthermore, the "routine use" exemption has been broadly construed in practice, constraining the 1974 Act's effectiveness as a meaningful constraint on the repurposing and sharing of personal information.[19]

The E-Government Act, by contrast, continued a shift towards greater institutionalization of privacy concerns initiated by the Clinton Administration, which had both directed executive departments and agencies to "designate a senior official within the agency to assume primary responsibility for privacy policy,"[20] and appointed a "chief counselor for privacy," within OMB.[21] The Act created additional decisionmaking process requirements, specifically that PIAs be conducted prior to the adoption of new technology, that they be reviewed by an agency's chief information officer or equivalent official, and that they be made available to the public online if "practicable."[22] It directed OMB to establish guidelines to ensure that PIAs are commensurate with the size of the information system, the sensitivity of information, and the privacy risk.[23] That guidance mandated that PIAs, in addition to providing a public description of the system, contain a risk assessment that specifically identifies and evaluates potential threats to individual privacy, discusses alternatives and identifies appropriate risk mitigation measures for each, articulates the rationale for the final design, and identifies what choices the agency made "as a result of performing the PIA."[24] The guidance further provides that PIAs be submitted to OMB as part of the agency budget review process.[25]

---

18 See 5 USC § 552a(e)(3)–(4), (6).

19 See, for example, Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law* 95–100 (1996) (discussing federal agencies' broad interpretation of the routine use exception and the limited effectiveness of courts in constraining these interpretations).

20 White House, *Memorandum on Privacy and Personal Information in Federal Records*, 34 Weekly Comp Pres Doc 870, 871 (May 14, 1998), online at http://www.whitehouse.gov/omb/memoranda/m99-05-a.html (visited Jan 12, 2008).

21 See White House, Press Release, *The Clinton-Gore Plan for Financial Privacy and Consumer Protection in the 21st Century* (May 4, 1999), online at http://clinton6.nara.gov/1999/05/1999-05-04-proposal-summary-on-financial-privacy-and-consumer-protection.html (visited Jan 12, 2008).

22 See 44 USC § 3501 note.

23 See id.

24 See OMB, *Guidance* at 4 (cited in note 8). The guidance further specified that PIA requirements apply not just to new information systems, but also when systems are converted from paper-based to electronic, when anonymous information is converted to an identifiable form, and when new uses of an existing IT system arise, including application of new technologies that significantly change how information is managed.

25 See id at 1 (imposing a deadline for PIAs for purposes of budgetary requests).

B. Inconsistent Implementation

Congress's inclusion of the PIA requirement engendered significant optimism. PIAs, the Senate Report stated, "are increasingly being recognized as an important means of ensuring that privacy protection is being taken into account."[26] Echoing that language, OMB Director Josh Bolten declared that PIAs—in combination with other existing requirements—would "ensure" that information "is handled in a manner that maximizes both privacy and security."[27] By both requiring agencies to weigh privacy concerns along with their primary substantive mandates and rendering their decision processes more transparent to outsiders, privacy advocates, in turn, believed PIAs would "force" agencies to "act responsibly . . . [and] ultimately lead to better-designed and more user-oriented government IT projects."[28]

The reality is far less uniform. The self-reported agency data in OMB's most recent report to Congress states that 12 percent of agencies did not yet even have written processes or policies for all listed aspects of PIAs, while 16 percent of systems that were admittedly covered by the PIA requirement did not have a complete or current PIA.[29] Particular laggards include agencies as diverse as the EPA (no compliant PIA for 50 percent of covered systems), the Office of Personnel Management (43 percent), the Department of Transportation (17 percent), and the Nuclear Regulatory Commission (52 percent), as well as the Departments of Defense (63 percent) and Homeland Security (76 percent). The incidence of noncompliance is likely even more worrisome in light of potential definitional problems. While the DOS reported that it had complete or current PIAs for 151 percent of its covered systems,[30] one half of the PIAs listed on their website are not publicly posted, and no PIAs have been issued for particularly privacy-sensitive programs such as PASS Card and other new border initiatives. Moreover, more individualized analyses suggest that these self-reported figures mask deeper qualitative noncompliance issues

---

26 S Rep No 107-74 at 28–29 (cited in note 5).

27 OMB, *Guidance* at 1 (cited in note 8).

28 Center for Democracy & Technology, *Statement of the Center for Democracy & Technology before the Senate Government Affairs Committee* (July 11, 2001), online at http://www.cdt.org/testimony/010711cdt.shtml (visited Jan 12, 2008) (arguing that the Privacy Act of 1974 had become obsolete and that PIAs could help reassure users of online government services).

29 See OMB, *FY 2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* 7, online at http://www.whitehouse.gov/omb/inforeg/reports/2006_fisma_report.pdf (visited Jan 12, 2008). Such figures are likely skewed even on their own terms, as they reflect the data from several agencies who, because of a difference in terminology, reported compliance over 100 percent, for example, Department of Agriculture (127 percent), DOS (151 percent), and Housing and Urban Development (254 percent). Id.

30 See id at 114–15.

with the PIA mandate. GAO reports, for example, have documented: (1) a number of specific failures to comply with privacy requirements for programs covered by the E-Government Act's terms;[31] (2) insufficient consideration of privacy concerns to satisfy the statute;[32] and (3) highly "uneven" compliance even with OMB's guidance on basic Privacy Act requirements.[33]

II. BARRIERS TO ACCOUNTABILITY IN PRIVACY DECISIONS

The inconsistent implementation of privacy processes provides a striking instance of the governance challenge created when Congress delegates substantial implementation discretion to administrative agencies. This challenge is heightened when the discretion delegated relates to the implementation of a secondary, rather than primary, objective of the agency. Legal scholars and political scientists have emphasized the capacity of the three constitutional branches of government to overcome the delegation problem and promote administrative accountability. Yet to date, traditional mechanisms for cabining delegated discretion have failed to yield consistent agency compliance with the statutory PIA mandate.

A. Limits of Process

The record of agency inconsistency belies the contentions that requiring a PIA process alone would "mandate" or "force" agency consideration of privacy values in decisions about technology. Certainly, in some circumstances Congress can successfully overcome the

---

31 See GAO, *Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs Are Developed* ("*Homeland Security Report*"), GAO-07-630T, 10–15 (Mar 2007), online at http://www.gao.gov/new.items/d07630t.pdf (visited Jan 12, 2008) (concluding that "DHS did not assess privacy risks in developing a data mining tool known as ADVISE ... as required by the E-Government Act of 2002," thereby creating the "risk that uses of ADVISE in systems containing personal information could require costly and potentially duplicative retrofitting at a later date to add the needed controls"). See also id at 18–19 (noting DHS's failure even to comply with Privacy Act notice for "Secure Flight," a program to evaluate passengers before they board an aircraft on domestic flights).

32 See GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866, 24–27 (Aug 2005), online at http://www.gao.gov/new.items/d05866.pdf (visited Jan 12, 2008) (noting that the IRS, Small Business Administration, and Risk Management Agency PIAs did not adequately address the statutory requirements regarding their data mining efforts and that the FBI conducted no PIA, in violation of agency regulations). See also GAO, *Homeland Security Report* at 17–18 (cited in note 31) (reporting that privacy guidelines developed for implementing the Intelligence Reform and Terrorism Prevention Act of 2004 "provide only a high-level framework for privacy protection").

33 See GAO, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304, 14 (June 2003), online at http://www.gao.gov/new.items/d03304.pdf (visited Jan 12, 2008) (reporting compliance with requirements as low as 70 percent).

principal-agent problems inherent in administrative delegation by, ex ante, employing specific statutory directives and requiring certain decision procedures.[34] Yet experience to date indicates that the PIA process requirement alone is insufficient to ensure the effective integration of privacy concerns.[35]

Indeed, external process requirements—without additional accountability or oversight structures—seem particularly unsuited to robust and consistent integration of values, like privacy, that may be at best orthogonal to, and at worst in tension with, an agency's primary mission. Of course, such secondary process mandates are intended explicitly to "mitigate agency tunnel vision or mission orientation" by requiring that they consider goals that are not directly within their charge.[36] Yet as a result, such mandates face particular problems with agency reluctance to comply. At a minimum, an agency's organic statute may embody a variety of goals—some that conflict directly with privacy concerns—to which administrators may legitimately point to in justifying their actions internally and externally.[37] More significantly, process directives alone may make little headway in redirecting agency structures, cultures, and decisionmaking routines geared to maximizing the agency's primary mission.[38]

Experience with the statute on which the PIA process was roughly modeled—the National Environmental Policy Act of 1969[39] (NEPA), which mandates the completion of environmental impact statements (EISs) for federal government action significantly affecting

---

34 See Matthew D. McCubbins and Talbot Page, *A Theory of Congressional Delegation*, in Mathew D. McCubbins and Terry Sullivan, eds, *Congress: Structure and Policy* 409, 411–13 (Cambridge 1987) (analyzing the tools Congress has at its disposal to control and channel agency decisionmaking and to improve information available to decisionmakers).

35 See, for example, David B. Spence, *Agency Discretion and the Dynamics of Procedural Reform*, 59 Pub Admin Rev 425, 436 (1999) (concluding that the Federal Energy Regulatory Commission used its discretion to minimize the effects of a series of imposed procedural requirements).

36 Jerry L. Mashaw, *Norms, Practices, and the Paradox of Difference: A Preliminary Inquiry into Agency Statutory Interpretation*, 57 Admin L Rev 501, 509 (2005) (arguing that agencies, like courts, must fit statutory language into the overarching legal framework).

37 See J.R. DeShazo and Jody Freeman, *Public Agencies as Lobbyists*, 105 Colum L Rev 2217, 2219 (2005) (discussing the tension between primary and secondary mandates). See also id at 2220 (citing examples of "[a]gencies frequently resolv[ing] [ ] interstatutory conflicts by prioritizing their primary mission and letting their secondary obligations fall by the wayside"); Jeanne Nienaber Clarke and Daniel C. McCool, *Staking Out the Terrain: Power Differential among Natural Resource Management Agencies* 4–5 (SUNY 2d ed 1996) (noting that some agencies may not easily incorporate the purposes of new legislation, even when they accord with the agency's original mission).

38 See generally Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking and Accountability in the Administrative State*, 56 Duke L J 377 (2006) (discussing systemic barriers to incorporating secondary goals in organizational decisionmaking).

39 Pub L No 91-190, 83 Stat 852, codified as amended at 42 USC §§ 4321–47 (2000).

environmental quality—exemplifies these concerns.[40] NEPA's initial focus on decision processes alone permitted widespread resistance in many agencies, resulting in widely inconsistent implementation,[41] and was, accordingly, subject to strong early criticism.[42]

NEPA is now, however, considered by many in and out of agencies to have successfully "institutionaliz[ed] environmental values in government."[43] Agency employees themselves attribute this transformation to the development of robust judicial and executive oversight unanticipated by the initial legislation. The text of NEPA provided for no oversight responsibility. Its drafters evidently assumed that the EIS requirement would be self-implementing, and the statute simply directed each agency to develop their own methods and procedures for integrating environmental values into agency decisionmaking. The year after the Act's passage, however, the oversight powers of the Council on Environmental Quality (CEQ) were enhanced by executive order.[44] The CEQ issued three sets of progressively more detailed implementation guidelines and took on a strong coordination role, working with agencies to direct consistent NEPA implementation.[45] At the same time, courts took an active role in review of the EIS process, ordering agencies to implement NEPA's procedural reforms, adopting broad constructions of many of the Act's provisions, and imposing meaningful sanctions for noncompliance in the form of costly and

---

40 See 42 USC § 4332(2)(C) (requiring EISs to report the environmental impacts of the proposed action, alternatives to the proposed action, and any adverse environmental impacts which cannot be avoided should the proposal be implemented).

41 See Allan F. Wichelman, *Administrative Agency Implementation of the National Environmental Policy Act of 1969: A Conceptual Framework for Explaining Differential Response*, 16 Nat Res J 263, 296–300 (1976) (studying the implementation of NEPA across twenty different federal agencies).

42 See, for example, Joseph L. Sax, *The (Unhappy) Truth about NEPA*, 26 Okla L Rev 239, 248 (1973) ("Until we are ready to face [ ] hard realities, we can expect laws like NEPA to produce little except fodder for law review writers and contracts for that newest of growth industries, environmental consulting.").

43 Serge Taylor, *Making Bureaucracies Think: The Environmental Impact Statement Strategy of Administrative Reform* 251 (Stanford 1984) ("Since the advent of NEPA, environmental concerns have been officially incorporated into every agency's charter."). See also Council on Environmental Quality, *The National Environmental Policy Act: A Study of Its Effectiveness after Twenty-Five Years* iii (Jan 1997), online at http://ceq.eh.doe.gov/nepa/nepa25fn.pdf (visited Jan 12, 2008) (discussing NEPA's "success" in making federal agencies take a "hard look" at the potential environmental consequences of their actions). But see Bradley C. Karkkainen, *Toward a Smarter NEPA: Monitoring and Managing Government's Environmental Performance*, 102 Colum L Rev 903, 904–06 (2002) (describing the positions of both proponents and critics of NEPA).

44 See Executive Order 11514, 35 Fed Reg 4247 (1970).

45 See Wichelman, 16 Nat Res J at 275–76 (cited in note 41) (discussing the CEQ's role as an overseer that provided "the coordination necessary to assure implementation of specific court decisions across the administrative process" and that became a focus to which agencies could turn voluntarily for informal guidance).

time-consuming injunctions and adverse publicity.[46] The resulting transparency, in turn, permitted public oversight by providing environmental advocates a window into agency decisionmaking. This combination of external oversight of the EIS requirement is credited for catalyzing a "wide range of internal agency adaptations," resulting in the integration of environmental concerns in agency decisions.[47]

B. Barriers to Oversight

In general, the president and Congress have important administrative oversight tools at their disposal. Advocates of presidential control of administration document the chief executive's capacity as primary administrative overseer,[48] citing his ability to overcome the interest group influence to which Congress and agencies are vulnerable[49] and to rationalize policy across agencies, encouraging the consistent administrative implementation of legal mandates.[50] Congress possesses, through its committee structure and budget oversight, the capacity to engage in either ongoing oversight of agency implementation of statutes—what political scientists call "police patrols"[51]—or more intermittent action prompted by the "fire alarms" sounded by "targeted beneficiaries as a mechanism to trigger formal investigations

---

46 Scholars point to judicial review as a particularly important element in NEPA's success. See, for example, Nicolas C. Yost and James W. Rubin, *Administrative Implementation of and Judicial Review under the National Environmental Policy Act*, in Sheldon M. Novick, Donald W. Stever, and Margaret G. Mellon, eds, 2 *The Law of Environmental Protection* ch 10:I (West 2007). See also *Kleppe v Sierra Club*, 427 US 390, 421 (1975) (Marshall concurring in part and dissenting in part) ("[T]his vaguely worded statute seems designed to serve as no more than a catalyst for development of a 'common law' of NEPA. To date, the courts have responded in just that manner and have created such a 'common law.' ... Indeed, that development is the source of NEPA's success.").

47 See Wichelman, 16 Nat Res J at 278 (cited in note 41) (describing initial resistance and eventual capitulation by agencies to EIS requirements).

48 See, for example, Elena Kagan, *Presidential Administration*, 114 Harv L Rev 2246, 2246–339 (2001) (arguing that presidents can press administrative agencies to act in ways they have not before, to address problems not previously seen, and to devise solutions not formerly contemplated); Cynthia R. Farina, *The "Chief Executive" and the Quiet Constitutional Revolution*, 49 Admin L Rev 179, 180–84 (1997) (discussing the evolution of constitutional law to permit extensive control of agencies by the chief executive and its impact on the "regulatory enterprise").

49 See, for example, William F. West, *Presidential Influence and the Coordination of Bureaucratic Policy: An Examination of the Doctrine of Executive Centralization* 23 (Bush School Working Paper No 520), online at http://bush.tamu.edu/research/workingpapers/wwest/TheTheoryofPresidentialManagement.pdf (visited Jan 12, 2008) (noting the increasing need for presidential mechanisms that reconcile differences among bureaucratic organizations due to the proliferation of interest groups).

50 See, for example, Stephen Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation* 71–72 (Harvard 1993) (discussing centralization by structuring agencies and using OMB review).

51 See Mathew D. McCubbins and Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols versus Fire Alarms*, 28 Am J Polit Sci 165, 166 (1984).

and/or legislative responses to noncompliance."[52] In addition to political controls on bureaucracy, judicial review can, as in the case of NEPA, provide a powerful independent check on administrative discretion.

We suggest, however, that several factors specific to the PIA context create obstacles to traditional forms of direct oversight by the political branches and the courts and hinder the public monitoring that can facilitate each: the contemporary politics of privacy, a lack of decision openness, and the opacity of decisions about technology.[53] Any policy prescription for privacy protection must contend with each.

1. Politics, secrecy, and technical impenetrability.

Expending political capital on privacy can be risky. While polls consistently reveal deep concern about information abuse and support for privacy protections in general,[54] particular policy decisions frequently counterpose privacy against two other powerful values: efficiency and security. The ideological and political pressures supporting each run deep. Technology is adopted, in large part, as a seemingly value-neutral means for promoting efficient and effective pursuit of public goals whose legitimacy has already been settled in the political arena. Seeking to overcome the resulting presumption in technology's favor with privacy claims exposes the bearer to political risk. Placing privacy in conflict with security raises even greater political hazard, because of the immense risk of even a low-probability security event. The experience of former Deputy Attorney General Jamie Gorelick, blamed for the set of directives creating a "wall" prohibiting FBI and CIA coordination in light of civil liberties concerns—an act former Attorney General John Ashcroft called "the single greatest structural cause for September 11"[55]—stands as a salient cautionary tale. As one

---

52 Matthew D. McCubbins, Roger G. Noll, and Barry R. Weingast, *Structure and Process, Politics and Policy: Administrative Arrangements and the Political Control of Agencies*, 75 Va L Rev 431, 434 (1989).

53 See generally Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U Pa L Rev 707 (1987) (discussing reasons why individual rights of action through the courts and executive and legislative oversight are insufficient to effect privacy protection with government, pointing to particular problems with access, technical knowledge, and intensity of supervision).

54 See, for example, Electronic Privacy Information Center (EPIC), *Public Opinion on Privacy*, online at http://www.epic.org/privacy/survey (visited Jan 12, 2008) (summarizing various public opinion polls on the importance of privacy and concluding that there is "strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities").

55 National Commission on Terrorist Attacks upon the United States, Tenth Public Hearing: Law Enforcement and the Intelligence Committee (Apr 13, 2004) (testimony of Attorney General John Ashcroft), online at http://www.9-11commission.gov/hearings/hearing10/ashcroft_statement.pdf (visited Jan 12, 2008).

news network reminded us, "no one wants to be the one who dropped the ball when, as predicted, terrorists strike again."[56]

These political disincentives are exacerbated by practical obstacles to robust oversight arising from limits on openness and transparency in the privacy assessment process.

The first obstacle inheres in the implementation of the E-Government Act itself. Despite the statute's explicit commitment to the production of PIAs before developing or purchasing IT systems, and the publication of those PIAs, it lacks any public consultation process for their production. Indeed, a federal court has rejected the single Freedom of Information Act[57] (FOIA) request by a privacy advocacy group for draft PIAs developed in advance of a proposed rulemaking on the very ground that those documents were "predecisional" and therefore fell within one of the established FOIA exemptions.[58] The politically charged nature of decisions balancing surveillance capacity with privacy safeguards further strengthens the incentives to take advantage of this shield. And while the safeguards afforded by the Administrative Procedure Act[59] (APA) at least permit some form of public participation in formal agency action effected by means of notice and comment rulemaking (albeit *after* the initial assessments have already been completed), the development or procurement of information systems is often treated as a management issue and accomplished through more informal means; in those contexts, if the PIA is not made available to the public prior to development or procurement, there is no vehicle for public participation before technology has been purchased and implemented.

The lack of explicit mechanisms for public participation in the PIA process—a process that, under the statute, should occur at the early stage of development—limits the opportunities for outside experts to assist the agency in identifying the privacy implications of often complex technological systems. Absent external direction or internal efforts to engage the public through a comment process or other means, public input is limited to the stage in which proposals and programs are well developed. Relegated to this late stage, the public com-

---

56 Thalia Assuras and Joie Chen, *House and Senate Committees Will Begin Rare August Hearings*, CBS News Transcripts (July 24, 2004) (discussing increased attention to intelligence reform following the release of the 9/11 Commission Report).

57 Pub L No 89-554, 80 Stat 383 (1966), codified as amended at 5 USC § 552 (2000 & Supp 2002).

58 See *EPIC v TSA*, 2006 WL 626925, *10 (DDC 2006) (rejecting a FOIA request by EPIC to obtain PIA associated with the development by the TSA of the Computer Assisted Passenger Prescreening System (CAPPS II)).

59 Pub L No 89-554, 80 Stat 381 (1966), codified as amended at 5 USC § 551 et seq (2000 & Supp 2004).

ments are more likely to result in revisions on the margins rather than fundamental switches in technology or architectural design.

A second constellation of transparency concerns arises from the technical nature of the information systems whose adoption the PIA process was designed to influence. In general, the problem of bureaucratic discretion increases along with information asymmetries between expert agencies and their overseers.[60] These asymmetries can be particularly pronounced because the debates that raise privacy concerns frequently involve technical standards that can be both procedurally and linguistically inaccessible.[61] Technology is often positioned as neutral with respect to values when, in fact, it can create and implement value decisions at least as effectively as more traditional forms of regulation.[62] Decisions about the design and deployment of technical systems, then, can permit bureaucrats to cloak policy decisions and mask the exercise of discretion behind claims of technical neutrality.[63] The problem is exacerbated by the fact that the privacy concerns created by information systems are frequently analyzed in the abstract and may depend upon testing an agency's specific—and often idiosyncratic—technological implementation. Unlike the type of expert information on which administrative policy more traditionally relies—the safe level of atmospheric chemical discharge, for example—privacy effects of system design have only recently become the

---

60 See Arthur Lupia and Mathew D. McCubbins, *The Democratic Dilemma* 79, 215–16 (Cambridge 1998) (highlighting the lack of common interest and information discrepancies between agents and principles).

61 See Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 Hastings L J 1321, 1380–81 (1992) (discussing the difficulty of congressional oversight in light of the growth in data processing as the source of privacy issues).

62 See Lawrence Lessig, *Code and Other Laws of Cyberspace* 107–08, 120–21 (Basic Books 1999) (noting the importance of structure in determining the ability of agencies to regulate and the danger that courts will back away from new and technical regulatory issues); Langdon Winner, *Do Artifacts Have Politics?*, in Donald MacKenzie and Judy Wajcman, eds, *The Social Shaping of Technology* 28–40 (Open 2d ed 1999) (discussing technology's impact on the structure of power and authority and its often inherently political nature); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex L Rev 553, 553–54 (1998) (arguing that technological capabilities and system design choices can impose rules on network participants, adding to or supplanting traditional forms of regulation); Helen Nissenbaum, *Values in the Design of Computer Systems*, 1998 Computers Socy 38, 38–39 (arguing that values, including public policy values, are embedded in design choices and asking who should control the undemocratic values embedded in designs).

63 See Winner, *Do Artifacts Have Politics?* at 31 (cited in note 62) (providing examples of political decisions cloaked as seemingly neutral aesthetic choices about architecture and city planning). As an example, systems of identification can be designed with a higher or lower propensity for false positives and false negatives. Depending upon the context of use, a decision to prefer errors in one direction or the other has profound policy consequences, for example, purging eligible voters from the rolls.

subject of regular public scientific analysis and often depend upon system-specific implementation details unknown to the public.[64]

Access to this information, however, is frequently obscured. The PIA and other public documentation of DOS's e-Passport program discussed below, for example, did not provide the exact specifications of the system under consideration, referring to a list of documents outlining both optional and mandatory requirements of standards developed by the International Civil Aviation Organization, a private standard-setting body. Nor did either agency proactively engage in scientific studies to identify systematically the privacy and security consequences of the technology or specific implementation options. Understanding the specifics of the technology DOS was seeking to employ—which is a prerequisite for meaningful participation in the notice and comment process accompanying its roll out—would have required a detailed analysis of the e-Passport proposal, access to and analysis of an enormous amount of free-standing technical documentation and specifications,[65] and, ideally, the ability to test the technology independently.

2. Anemic oversight.

Reflecting these obstacles, oversight of PIA agency implementation has been weak. The E-Government Act and guidance implementation appear to anticipate a central role for executive branch oversight by incorporating PIAs into OMB review, a principal means by which the White House has exercised political control over agency discretion and become much more directly involved in administrative action in recent decades.[66] Indeed, President Clinton's chief counselor

---

64 This might be a context in which adherence to the standards of the Data Quality Act, Pub L No 106-554, 114 Stat 2763 (2000), codified at 44 § USC 3516 note (2000), could possibly be helpful, as it could force agencies to provide research support for privacy and security claims. Such a requirement could, of course, cut in the opposite direction.

65 See Marci Meingast, Jennifer King, and Deirdre K. Mulligan, *Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport*, Proceedings of IEEE International Conference on RFID 4–5 (2007), online at http://www.truststc.org/pubs/157/Meingast_King_Mulligan_RFID2007_Final.pdf (visited Jan 12, 2008) (discussing the e-Passport project's failure to address security and privacy risks to passport holders, in part because of insufficient information).

66 It has done so by means of "regulatory review." See Executive Order 12866, 58 Fed Reg 51735 (1993) (establishing the guiding principles agencies must follow when developing regulations). See also GAO, *Rulemaking: OMB's Role in Reviews of Agencies' Draft Rules and the Transparency of Those Reviews*, GAO-03-929, 110 (Sept 2003), online at http://www.gao.gov/new.items/d03929.pdf (visited Jan 12, 2008) (concluding that while Office of Information and Regulatory Affairs reviews clearly have an analytical component, they also are a way to ensure tbat agencies' regulatory programs are consistent with administration priorities); Steven Croley, *White House Review of Agency Rulemaking: An Empirical Investigation*, 70 U Chi L Rev 821, 846–49 (2003) (examining nearly twenty years of OMB review of agency rulemaking).

for privacy at OMB, Peter Swire, a political appointee who enjoyed close relations to the White House and participated in a wide range of policymaking activity,[67] considers the OMB review process a critical intervention point for establishing cross-agency privacy policy.[68] Executive oversight, however, has not emerged as a means for ensuring that agencies consider privacy in the Bush presidency—a presidency strongly aligned with security rhetoric above all else—highlighting political accountability's contingency on a particular administration's commitment to the operative statutory goal. After taking office, President Bush did not preserve the chief privacy counsel position in OMB despite calls for a renewal of the position by advocacy groups.[69] To date, privacy issues at OMB have been delegated to a policy analyst who lacks the ability to intervene at a policy level and has limited authority to challenge agency noncompliance with privacy mandates absent substantial support from higher agency personnel. OMB further signaled a low level of commitment to privacy oversight by failing to provide the PIA guidance mandated by Congress until seven months after the statute's operative date,[70] subsequently encouraging agencies to make PIAs available only *after* agency budgets are finalized, and undermining the intended use of PIAs as a predecisional privacy input and a potential, if weak, vehicle for public feedback. The decision not to place privacy under the purview of a high-level official is particularly detrimental in the context of OMB, which, hindered by resource constraints and competing priorities, is often ineffective at proactive coordination of consistent action across executive agencies in any circumstance.[71] The result has been, in the words of the GAO, a

---

67 His work has spanned encryption policy, the creation of privacy policies on federal government web sites, and medical records privacy. See Peter P. Swire, *The Administration Response to the Challenges of Protecting Privacy* 14, 17 (unpublished manuscript, presented at the Stanford Law Review Symposium on Privacy, Jan 8, 2000), online at http://www.peterswire.net/stanford7.doc (visited Jan 12, 2008).

68 See id at 22.

69 See Center for Democracy & Technology, Press Release, *Public Interest Groups and Academics Call on Bush Administration to Fill Privacy Position* (Apr 16, 2001), online at http://www.cdt.org/press/010416press.shtml (visited Jan 12, 2008) (reporting on concern from privacy advocacy groups over the vacant position).

70 Agencies were to begin producing PIAs in April 2003, 120 days after enactment, but OMB did not issue its guidance until September of that year. See generally OMB, *Guidance* (cited in note 8).

71 See William F. West, *Presidential Leadership and Administrative Coordination: Examining the Theory of a Unified Executive*, 36 Pres Stud Q 433, 445–46 (2006) (noting that OMB does not engage in proactive oversight intended to reduce conflicts among regulations or to ensure consistent application of the regulatory analysis process); Lisa Schultz Bressman and Michael P. Vandenbergh, *Inside the Administrative State: A Critical Look at the Practice of Presidential Control*, 105 Mich L Rev 47, 50 (2006) (arguing that review does not successfully avoid inconsistencies among the regulations of a particular agency).

"lack of sufficient OMB leadership [and] guidance" on privacy compliance generally.[72]

These barriers to PIA oversight also amplify disincentives for legislative action. The attendant political risks and the strength of interest groups typically aligned against privacy legislation enhance the difficulty and cost of sustaining a coalition committed to active congressional monitoring of statutory implementation after passage.[73] The practical challenge of monitoring privacy and technology choices—especially after the elimination of Congress's Office of Technology Assessment in 1995[74]—under a system in which particular committees and subcommittees frequently oversee only one or a few agencies, may make active congressional policing a particularly inefficient means for oversight of a cross-agency mandate. The opacity of administrative privacy and technology decisionmaking diminishes the public's access to information necessary to raise the alarm for congressional action. Not surprisingly, while GAO—Congress's oversight arm—has issued a number of reports criticizing privacy decisions ex post, Congress itself has not engaged, on the whole, actively in monitoring.[75]

---

72 GAO, *Privacy Act* at 40 (cited in note 33).

73 See Priscilla M. Regan, *Legislating Privacy: Technology, Social Value, and Public Policy* 207–09 (UNC 1995).

74 See Office of Technology Assessment (OTA), *OTA Archive* (Aug 1996), online at http://www.gpo.gov/ota (visited Jan 12, 2008):

> For 23 years, the nonpartisan analytical agency assisted Congress with the complex and highly technical issues that increasingly affect our society.... The 104th Congress voted to withdraw funding for OTA and its full-time staff of 143 persons, and cover only a skeleton staff and the amount needed for the agency's final closeout.

75 An October 2007 Lexis search of the "Congressional Record" database over the past ten years for "privacy impact assessment" yields forty-nine hits; there are no colloquies or discussion of PIAs on the floor, and most of these hits are mentions in passing, or texts of bills and amendments. Only two hearings have even included any sustained discussion of PIAs, both in colloquy with DHS privacy officers. See Protection of Privacy in the DHS Intelligence Enterprise, Hearings before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the House Homeland Security Committee, 109th Cong, 2d Sess (2006) (testimony of Maureen Cooney, Acting Chief Privacy Officer, Department of Homeland Security) (describing how "the Privacy Office has worked to build privacy into the sinews of" DHS); Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security, Hearings before the Subcommittee of Commercial and Administrative Law of the House Committee on the Judiciary, 108th Cong, 2d Sess (2004) (discussing the unavailability of PIAs for meaningful notice and comment). However, Senator Lieberman, author of the E-Government Act of 2002, and his staff have engaged in some oversight activities, the majority of which occurred at the staff level and off the public record. Some of the Senator's work in this area is evident in press releases. See, for example, Senate Committee on Homeland Security and Governmental Affairs, Press Release, *DHS Violates Privacy Impact Requirements with US Visit Technology* (Dec 4, 2003), online at http://www.hsgac.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=599&Affiliation=C (visited Jan 12, 2008) (reporting Senator Lieberman's correspondence with then–DHS Secretary Tom Ridge and raising DHS's failure to conduct and make public privacy impact assessments for biometric technology); Senate Committee on Homeland Security

Finally, not a single court challenge has been brought against a PIA to date. There is certainly a possibility that effective judicial oversight may germinate in a contingent and unexpected manner as it did with NEPA. Yet, scholars underscore, as well, the ways in which similar problems of access, technical knowledge, and required intensity of supervision undermine individual rights of action.[76] Moreover, it may well be that the E-Government Act and guidance as written simply will not provide the traction for review found in the far more detailed iterations of the NEPA rules.

III. SEEKING ELEMENTS OF ADMINISTRATIVE SUCCESS: THE CASE OF RFID

The inconsistency of PIA implementation is epitomized by the cases of two different agencies—DOS in the case of the e-Passport program and DHS with respect to its US-VISIT initiative—considering the adoption of RFID technology in travel documents. This Part explores some of the elements salient to the DHS US-VISIT process, including agency structure and personnel that might explain that process's relative success in contrast to DOS's comparable inquiry. Together with the preceding discussion of oversight obstacles, these case-specific compliance experiences can suggest factors to overcome and elements to reproduce in the future institutionalization of privacy policy.

A. The Cases in Brief

1. The e-Passport program.

In February 2005, DOS published a proposed rulemaking setting forth a program for an e-Passport, an enhanced version of the traditional passport featuring an embedded electronic chip containing the information from the data page of the passport and a digital copy of the bearer's photo. The chip, a radio frequency (RF) transponder, is readable without physical contact through wireless technology. The agency concluded the previous year that the e-Passport would provide "significant security benefits" in that it was more tamper-resistant and

---

and Governmental Affairs, Press Release, *Government Privacy Protections Fall Short, Lieberman Calls for Leadership, Greater Commitment of Resources* (July 30, 2003), online at http://www.hsgac.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=333&Affiliation=C (visited Jan 12, 2008) (reporting Senator Lieberman's criticism of the GAO for failing to protect privacy rights and his call to the Bush Administration to show a greater commitment to privacy policy).

76 See, for example, Simitis, 135 U Pa L Rev at 746 (cited in note 53) ("For a democratic society [ ] the risks [of processing personal data] are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy.").

harder to forge than traditional passports.[77] Yet the proposed rule—a product of a two-year process—and the summary PIA made public after it had been promulgated failed to address privacy (and security) risks to the bearer whose personal information the RFID chips contained.[78] Indeed, the two-page PIA omits most of the critical elements specified in the OMB guidance; notably, it does not mention RFID technology, it neither identifies nor addresses any potential privacy risks it might create, and it provides no information about the range of testing, let alone the data that informed DOS's technical decisions.[79] The proposed rule itself, without considering the effect of technology on data access and collection, summarily rejected data protection concerns, concluding that the e-Passport did not merit encryption because "the personal data stored on the passport's electronic chip consists simply of the information traditionally and visibly displayed on the passport data page."[80]

This silence on risks is particularly striking in light of the threat inherent in RFID technology. Indeed, documents later received pursuant to a FOIA request document internal DOS discussions about concerns over "skimming"—unauthorized wireless access of the data on the transponder without the owner's knowledge or consent—as early as January 2003, yet tests to examine the e-Passport's vulnerability were not requisitioned until February 2005, several months after the PIA was completed.[81] The results of those tests, performed by the National Institute of Standards and Technology, have still not been released to the public at the time of publication.[82] While skimming in and of itself poses privacy problems inherent in the access to personally identifiable data and photographs, the fact that the vulnerable

---

77 See DOS, *Abstract of Concept of Operations for the Integration of Contactless Chip in the U.S. Passport* 3, 28 (2004), online at http://www.statewatch.org/news/2004/jul/us-biometric-passport-original.pdf (visited Jan 12, 2008).

78 Meingast, King, and Mulligan, *Embedded RFID and Everyday Things* at 4 (cited in note 65). See generally DOS, *2006 Summary Privacy Impact Assessment* (2004), online at http://foia.state.gov/spias/20061.dos.pia.summary.passport-cleared.pdf (visited Jan 12, 2008).

79 Compare DOS, *2006 Summary Privacy Impact Assessment* (cited in note 78), with OMB, *Guidance* (cited in note 8) (setting out PIA content requirements). The Center for Democracy & Technology has sought, as has the Samuelson Law, Technology & Public Policy Clinic and the ACLU, access to PIAs conducted in relation to the e-Passport project. At this point we believe it is quite possible that a full PIA was not conducted, and if it was, it seems highly likely that it occurred after the development of the system rather than before as directed by the law. See Letter from Center for Democracy & Technology to Condoleezza Rice, Secretary of State, 1–2 (May 2, 2007), online at http://www.cdt.org/security/identity/20070502rice.pdf (visited Jan 12, 2008).

80 DOS, *Electronic Passport*, 70 Fed Reg 8305, 8306 (2005) (proposed rule).

81 See Meingast, King, and Mulligan, *Embedded RFID and Everyday Things* at 2 (cited in note 65).

82 They have also not been released to one of the authors under a still-pending FOIA request.

data is frequently attached to a physical person (the carrier) magnifies the security threat. Passport bearers can be tracked, identified, and subject to violence triggered remotely by as little information as their US nationality. While some of the privacy concerns were ultimately addressed in a revised final rule (specifically the incorporation of an antiskimming material in the cover of the passport, a locking code limiting data access to authorized readers, and transmission encryption), the ultimate rollout of the program was delayed a year. Moreover, the question of whether RFID was the appropriate technology, balancing the costs and effectiveness of privacy protection add-ons, was never addressed in the first instance.

2. The US-VISIT program.

DHS chose similar RF technology when piloting the US-VISIT program pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004.[83] That statute required DHS to collect biometric exit data from all individuals who are also required to provide such data when they enter the United States, and DHS proposed the use of passive RFID tags embedded in the I-94 arrival/departure form to track entry and exit of foreign visitors at land border point of entry crossings. The embedded tag would store no personally identifiable data, but would instead contain a unique identifier linked to a traveler's information in the US-VISIT database.[84]

The two PIAs DHS conducted for the US-VISIT project are eight and thirty-three pages long respectively.[85] They contain relatively detailed information about the system architecture, data flows, and access controls, and lay out the privacy threats and mitigation techniques in clear charts. While the PIA process was not entirely without criticism of its timing and substantive conclusions,[86] it was generally lauded as "a high-quality PIA" that can "serve as a model for upcoming PIAs of other national security–related systems."[87] To further ad-

---

83 Pub L No 108-458, 118 Stat 3638.

84 See DHS, *Privacy Act of 1974; Systems of Records* 2 (July 1, 2005), online at http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_usvisit_aidms.pdf (visited Jan 12, 2008).

85 See generally DHS, *Privacy Impact Assessment and Privacy Policy; US-VISIT Program*, 69 Fed Reg 2608 (2004); DHS, *US-VISIT Program, Increment 2 Privacy Impact Assessment in Conjunction with the Interim Final Rule of August 31, 2004* (2004), online at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf (visited Jan 12, 2008).

86 See Senate Committee on Homeland Security and Governmental Affairs, *Government Privacy Protections Fall Short* (cited in note 75) ("In order for the privacy impact assessment to serve its intended purpose, the PIA must be conducted before the agency develops or procures information technology for the program.").

87 Letter from Center for Democracy & Technology to DHS Privacy Office 4 (Feb 4, 2004), online at http://cdt.org/security/usvisit/20040204cdt.pdf (visited Jan 12, 2008).

vance public participation in the PIA process, the DHS chief privacy officer (CPO) held meetings with privacy and immigration organizations to further explore privacy concerns. Issues identified through these meetings, and by experts' comments on the PIA, were reflected in subsequent PIAs and in the ultimate design of the project.[88]

B. Possible Explanations

A rich literature on decisionmaking in organizations documents the difficulty inherent in attempts to force groups to include new priorities—especially those imposed from the outside—in their program goals.[89] Organizations are largely structured to foster the pursuit of preexisting interests, which in the case of agencies is their primary statutory mandate. Those interests are reflected in the relative power and status accorded different individuals and groups; the way substantive tasks are allocated to different units; the expertise, background, and priorities of the organization's members; and the existing rules—formal and informal—governing decisionmaking. Each of these elements creates systemic resistance to changes in priorities.

Delving further into the differential experience of the DOS and DHS privacy processes surrounding RFID adoption, this Part draws tentative lessons as to the elements that may overcome obstacles to the incorporation of privacy concerns into agency decisionmaking. Faced with an identical mandate and executive guidance on PIAs and similarly freed from vigorous oversight, what might explain the differences in agency behavior, and more specifically DHS's engagement in practices that met, and in many respects exceeded, compliance?

The RFID case studies suggest three areas of significant variance between the agencies—each consistent with the broader literature concerning internal and external forces on compliance within the pub-

---

88 See Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security, Hearings before the Subcommittee on Commercial and Administrative Law of the House Committee on the Judiciary, 108th Cong, 2d Sess (2004) (testimony of James X. Dempsey, Executive Director, Center for Democracy & Technology) ("Dempsey Testimony") (reporting that advocates expressed their concerns about issues such as the lack of information on redress issues for visitors who believe that information held about them may be incorrect or incorrectly interpreted and the unclear nature of the data quality and data retention rules).

89 See, for example, DeShazo and Freeman, 105 Colum L Rev at 2220–21 (cited in note 37) (exploring the problem of agency reluctance in the face of multiple mandates and explaining how and why agencies might resist secondary mandates, "which typically—though not always—come in the form of obligations imposed in separate statutes passed after Congress delegates the agency's primary mission in its enabling law"); Clarke and McCool, *Staking Out the Terrain* at 45 (cited in note 37) (explaining that agencies may not easily integrate functions and purposes of new legislation even when they accord with agencies' original missions). See also Taylor, *Making Bureaucracies Think* at 93–169 (cited in note 43) (providing case studies of how NEPA was implemented and resisted by the Forest Service and the Army Corps of Engineers).

lic and private sector—that we identify as potentially contributing to the disparate levels of compliance with the PIA mandate: (1) the status and independence of a privacy expert embedded within the agency; (2) the decentralized distribution, disciplinary diversity, prior experience, and expertise of the privacy staff; and (3) the creation of an alternative external oversight structure, which proved particularly significant given the lack of systematic congressional and administrative privacy oversight.

1. Status and independence of embedded privacy experts.

The most visible difference between the two agencies at the time of the RFID PIA processes was the existence of a high-status privacy expert within DHS, the agency CPO, specifically charged with advancing privacy among competing agency interests, located in a central position within the agency decisionmaking structure, drawing on internal relationships and external sources of power, and able to operate with relative independence. The existence of such an embedded expert was not fully predetermined by statute or agency culture, but resulted instead from the confluence of structural, personal, and contextual contingent factors. Nonetheless, the status and independence proved determinative in the compliance—and "beyond compliance"—choices surrounding the US-VISIT program.

The statute that established DHS provided the basic predicate for these developments. The Homeland Security Act of 2002[90] ("DHS Act"), which consolidated numerous previously independent intelligence, regulatory, and enforcement functions under the cabinet-level DHS, specifically established a privacy officer within the agency, the first statutory privacy officer position at the federal level in the United States.[91] The legislation directed the secretary of homeland security to appoint a senior official with broad responsibility for ensuring that the use of technologies sustain, and do not erode, privacy protections; ensuring compliance with the Privacy Act of 1974; evaluating legislative and regulatory proposals involving personal information; and conducting privacy impact assessments.[92]

In response to his statutory mandate, Secretary Tom Ridge appointed Nuala O'Connor Kelly, then-CPO of the Department of Commerce, as CPO at DHS. Kelly was a respected professional in the privacy community, having served previously at the technology company DoubleClick, and one of the founding members of the Interna-

---

90 Pub L No 107-296, 116 Stat 2135.

91 See 6 USCA § 142 (2007).

92 See id.

tional Association of Privacy Professionals, an industry group that promulgates best practices, provides privacy professional certifications, and advocates on privacy issues among public and private bodies. Kelly enjoyed a high level of visibility and support from Secretary Ridge, reported directly to him, and was part of his senior leadership team.

These developments occurred against a backdrop of organizational fluidity. While individual preexisting agencies and offices included within the new DHS umbrella may have brought with them strong cultures, practices, and priorities, the new DHS CPO office and its first occupant developed alongside the new routines, cultural presumptions, and working relationships negotiated more broadly within the newly organized DHS and its leadership. Because of a combination of internal agency structure mandated by external statutory mandate, Kelly's experience as a respected professional in the privacy community, and her legitimacy as a result of Secretary Ridge's commitment to privacy issues generally and to his appointee in particular, DHS had a privacy oversight function characterized by legitimacy and strength from its inception.

Kelly, moreover, used the relative autonomy provided by the status of her appointment, as well as the trust invested in her by Secretary Ridge, to reframe DHS's agency mission to include the privacy goals embodied by her office. Relying on arguably ambiguous language in the DHS Act discussing annual CPO reporting to Congress[93] and on thin legislative history,[94] Kelly, with Secretary Ridge's support, put forth a forward-leaning interpretation of her office's independence. She took a number of steps to institutionalize her office's autonomy and independence from both the secretary and other executive branch controls, particularly the OMB clearance process. In particular, Kelly framed her office's direct-congressional-reporting function as both a right and an obligation, and emphasized the function's impor-

---

93 The statute directs the privacy officer to assume primary responsibility for privacy policy, including "preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters." 6 USCA § 142(a)(6). In other instances, however, Congress has more clearly created direct reporting obligations. For example, in creating the Privacy and Civil Liberties Oversight Board, Congress explicitly created an independent reporting requirement stating, "the Board shall prepare a report to Congress." Intelligence Reform and Terrorism Prevention Act of 2004 § 1061(c)(4), 118 Stat at 3684, codified at 5 USC § 601 note (2000 & Supp 2004).

94 See Administrative Law, Adjudicatory Issues, and Privacy Ramifications of Creating the Department of Homeland Security, Hearings before the Subcommittee on Commercial and Administrative Law of the House Committee on the Judiciary, 107th Cong, 2d Sess 2–6 (2002) (testimony of Peter P. Swire, Professor of Law, Ohio State University) (criticizing the Homeland Security Act of 2002 as "all accelerator and no brakes" and as imposing extra layers of bureaucracy that will impede information gathering).

tance as a signal of structural independence. She took the position that reports from her office should not be reviewed by the DHS secretary nor go through the standard OMB policy review process, and during her tenure Kelly successfully prevented DHS or the White House from exercising editorial control over reports issued by her office or privacy impact assessments, although her annual report did go through a review.[95] Through this interpretation, moreover, she sought opportunities to speak directly to potential oversight bodies—construed broadly to include Congress, the press, and the public—even when her communications and reports showed the agency failing in its obligation to protect privacy. In particular, the ability to point to external pressures, and use an external reporting mechanism both as a threat and a means for inviting external oversight, provided particularly effective means for enhancing legitimacy within the organization,[96] tools that would be used to great effect during the period of the US-VISIT privacy process. Finally, Kelly leveraged her status and independence so as to play a singular role in the creation of the Data Privacy and Integrity Advisory Committee (DPIAC), an external oversight body discussed below, which played an important role in the depth of the US-VISIT PIA process.

None of the individuals who can be said to be responsible for spearheading privacy policy at the DOS had the status or the independence of Kelly. The senior DOS official designated as responsible for privacy matters is not a dedicated CPO, but the assistant secretary for administration—a high-level position, no doubt, but one differently situated with respect to overseeing and operationalizing the privacy mandate at DOS. Indeed, the position was held by William A. Eaton, a career foreign service officer, from July 2001 through May 2005, when he was confirmed as US Ambassador to Panama, after which the post was vacant for over a year.[97] Formal privacy compliance activities are managed and overseen by civil servants, some of whom have substantial and impressive experience with privacy,[98] but none of whom possess comparable status or authority to the DHS CPO.[99]

---

95 Telephone interview with Nuala O'Connor Kelly, former DHS CPO ("Kelly Interview") (June 1, 2007).

96 See Jeffrey Pfeffer and Gerald Salancik, *The External Control of Organizations: A Resource Dependence Perspective* 72–78 (Harper and Row 1978) (describing the interplay between an organization's external "environments" and the way it focuses attention internally).

97 See DOS, *Assistant Secretaries of State for Administration*, online at http://www.state.gov/r/pa/ho/po/12108.htm (visited Jan 12, 2008).

98 See Dempsey Testimony (cited in note 88).

99 See Swire, *The Administration Response* at 22 (cited in note 67) (concluding, based on his experience as the first Chief Counselor for Privacy that "privacy debates have a significant

Because of these structures, neither high-level officials for whom privacy tasks are grafted on to existing responsibilities nor civil service privacy compliance officers are likely to possess means to achieve a comparable level of independence as did the DHS CPO. The former are senior officers "designated" as responsible for privacy pursuant to the framework established in the Clinton Administration and codified by the Consolidated Appropriations Act, 2005;[100] the very language signals the subordinate status of the privacy function.

The "designated" privacy officer structure, in contrast to that developed at DHS, further undermines privacy officers' ability to draw legitimacy from external pressures. Specifically, designated officers are instructed to issue reports regarding the treatment of personally identifiable information to an intermediate entity within their own agency: the inspector general. This precludes any independent relationship with Congress through which they could enlist such an external, legitimacy-enhancing oversight function. While the DHS CPO, furthermore, might take advantage of OMB's lack of interest in privacy, the absence of executive oversight resulting from President Bush's removal of the high-level centralized policy management function from within OMB[101] both limits pressure on other agencies' privacy officers to perform PIAs and also reduces the power of individual privacy officers to respond to agency resistance by pointing to external requirements to bolster their internal legitimacy.

The DHS experience underscores scholarship that emphasizes independence in action and reporting as essential components of effective government data-protection offices.[102] In the case of DHS at

---

political dimension, and there are advantages to having a political appointee rather than a civil servant articulate the privacy issues, both within the Administration and in public").

100 Pub L No 108-447, 118 Stat 2809, 3268–70, codified at 5 USC § 552(a) note.

101 See the Center for Democracy & Technology, *Public Interest Groups and Academics* (cited in note 69).

102 See, for example, Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-regulatory Privacy Protection Board*, 54 Hastings L J 1183, 1208–10 (2003) (emphasizing the importance of independence for the success of the Privacy Protection Board); Letter from Center for Democracy & Technology to OMB Information Policy Committee (July 29, 1997), online at http://www.cdt.org/privacy/ntia.html (visited Jan 12, 2008) (recommending a body for privacy oversight that would be "an independent voice empowered with the scope, expertise, and authority to guide public policy"); Schwartz, 43 Hastings L J at 1379–84 (cited in note 61) (arguing that an independent data protection body could develop expertise and specialization currently missing in congressional oversight); David H. Flaherty, *Protecting Privacy in Surveillance Societies* 381 (UNC 1989) (concluding that independent agency oversight is "essential" to make a data protection law work in practice); Simitis, 135 U Pa L Rev at 742 (cited in note 53) ("Efficient regulation presupposes the establishment of an independent control authority. Experience confirms what was argued in the earliest debates: a mandatory framework for data processing is not sufficient."); Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and*

the time of the US-VISIT PIA, that independence enabled the CPO to argue that privacy was an integral component of the institution's core mission.[103] It enabled the CPO to act relatively autonomously, particularly with respect to issuing reports on agency actions and investigations, thereby establishing an independent voice and relationships with external oversight bodies. Finally, it provided the political capital and access necessary to create a new independent, external quasi-oversight mechanism comprised of privacy and security experts, thereby securing an additional mechanism to ensure that agency actions and commitments affecting privacy were examined. These three actions were likely heavily dependent on the status of the CPO and in turn positively influenced the US-VISIT PIAs and other work of the office.[104]

2. Expert personnel, integrated structure, and the PIA tool.

Kelly further leveraged her individual capacity to affect decisionmaking within the agency through decisions about both personnel and structure. In particular, Kelly both assembled a staff of demonstrated privacy professionals with diverse disciplinary skills and located these employees not only in the central DHS privacy office, but embedded them as well within the operational units throughout the agency. This combination of privacy expertise, varied training and perspective, and decentralized integration throughout decisionmaking structures, was particularly well suited to take advantage of the privacy impact assessment mechanism, an inherently interdisciplinary tool for affecting decisionmaking from the "bottom up."

Like Kelly, several key privacy office staff had held prior positions that required them to identify emerging privacy issues proactively and engage a wide range of businesses in the development of privacy policy and implementation of privacy management strategies.[105] Several staff members had been involved in negotiations with

---

the Rights of Citizens 42–43 (1973) (concluding that agency oversight was the strongest option for protecting privacy but rejecting it due to lack of political support).

103 In fact, OMB guidance left it up to the agency whether to conduct a PIA at all where the personal information at issue was about aliens. See OMB, *Guidance* (cited in note 8) ("Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.").

104 A study of environmental regulation found that the effectiveness of the unit charged with environmental protection depends on its own commitment to the program, its autonomy, the outside support for its efforts, and the clarity of its goals. See Taylor, *Making Bureaucracies Think* at 252 (cited in note 43) (discussing requirements for agency institutionalization of environmental values).

105 For example, Maureen Cooney, Chief of Staff and Director of International Privacy Policy, was Legal Advisor for International Consumer Protection at the FTC where she worked on international privacy and security issues; Elizabeth Whitnell, Chief Counsel to the Privacy Office, was a lawyer at the Office of Information and Privacy at the DOJ; Peter Sand, Director of

the European Union about the adequacy of United States privacy law and practice, which provided them with a deep familiarity with the larger trade and political context of agency privacy decisions. Kelly specifically identified the breadth of her core privacy staff—lawyers, technologists, government insiders, implementation and education experts—and their connections and experiences as essential to the success of the office.[106] Unlike other agencies' CPO offices, which grew out of the compliance-focused Privacy Act and Freedom of Information Act offices, the DHS CPO office was staffed with individuals who possessed the inclination and capacity to build on the opportunity presented by the PIA process to identify problems with emerging technology, distinguish policy tradeoffs in technology design choices, and present alternative strategies.

Several members of the DHS CPO staff, moreover, were active participants in professional associations and conferences.[107] The growth of professional organizations in the privacy field—some aimed at self-regulation, some at information sharing, and some at the creation of a professional field—has played an important role in defining the activities and standards to which CPOs should aspire.[108] The influence of privacy professionals on one another, and the relative weight placed on the policies and practices of others is increased by the relatively ambiguous nature of success in this volatile but thinly regulated

---

Privacy Technology, was the Chief Privacy and Information Officer for the Pennsylvania Office of the Attorney General; Toby Levin, the Senior Advisor to the Department of Homeland Security Privacy Office, was a Senior Attorney in the Division of Financial Practices at the FTC, where she worked on children's privacy and financial privacy, among other issues; and Rebecca Richards, Director of Privacy Compliance at the Department of Homeland Security, was Director of Policy and Compliance at a privacy certification program (TRUSTe) and worked on the US–European Union Safe Harbor accord while an international trade specialist at the US Department of Commerce.

106 See Kelly Interview (cited in note 95).

107 Members of the Privacy Office were regular presenters at meetings of the International Association of Privacy Professionals (IAPP), the leading privacy professional association. For example, Nuala O'Connor Kelly was the keynote at the IAPP 2004 Privacy and Data Security Summit and Exposition; Rebecca Richards and Lisa Dean, Privacy Officers at the TSA, part of DHS, both spoke at the 2005 IAPP summit; and this summer Senior Privacy Advisor Toby Levin, International Privacy Policy Director John Kropf, Privacy Technology Director Peter Sand, and Privacy Compliance Director Rebecca Richards all participated in a panel discussion at the IAPP Privacy Summit 2007.

108 The professionalization of a field often yields what has been termed "normative isomorphism," the standardizing effect that professional training, education, and networks exert on organizational behavior. See Paul J. DiMaggio and Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 Am Soc Rev 147, 152–53 (1983) (describing how professionals in a field look for candidates similar to themselves when doing new hiring). In interviews conducted for the authors' larger study of corporate Chief Privacy Officers, *Catalyzing Privacy: Comprehensive Compliance Regimes under Incomplete Law* (cited in note 1), privacy officers routinely point to their peers and professional privacy organizations as important sources that inform their own and their institutions approach to privacy.

area.[109] The lack of inherent substantive standards for measurement in the privacy arena creates greater dependence upon peers and professional associations for direction, metrics, and validation. The importation of experts with substantial ties to the broader privacy community brought a strong emphasis on detailed risk analysis and issue identification into the PIA structure at DHS, developed through information sharing with peers and past professional experience. The expectations of the broader privacy community became a source of external input and pressure, as well as a source of knowledge and a forum for iterative program design, on the DHS CPO through the office's employees' ties to this community.

Kelly believed it essential to embed privacy personnel within the operational units of DHS, and, in addition to her core privacy staff, each of the operational divisions—and even particular programs that raised heightened privacy concerns, such as US-VISIT—had dedicated privacy officers.[110] Privacy professionals in the private sector interviewed by the authors, as well as other privacy professionals, stress the importance of embedding expertise within business units and establishing specific staff who are personally responsible for privacy—typically through indirect reporting mechanisms—as essential to operationalizing privacy in large decentralized organizations.[111] Literature on the relationship between formal structures and successful de-

---

[109] A second form of isomorphism, "mimetic isomorphism," results from uncertainty. Where goals are ambiguous and success difficult to measure, organizations will more readily tend toward imitating others in the field who appear to be successful. This mimicry in the face of uncertainty appears to be another substantial force in standardizing organizational responses to issues such as privacy. See DiMaggio and Powell, 48 Am Soc Rev at 151–52 (cited in note 108) (noting that organizations tend to model themselves after similar organizations in their field that they perceive to be more legitimate or successful). This effect also finds support in the authors' ongoing study of CPOs.

[110] See, for example, DHS, *Naturalization Redesign Test Pilot Privacy Impact Assessment* (2007), online at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_nrtp.pdf (visited Jan 12, 2008); TSA, *Airport Access Control Pilot Project Privacy Impact Assessment* 6 (2004), online at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_aacpp.pdf (visited Jan 12, 2008); DHS, *US-VISIT Program* at 10 (cited in note 85).

[111] See Kelly Interview (cited in note 95); Bamberger and Mulligan, *Catalyzing Privacy* (cited in note 1); David H. Flaherty, *Privacy Impact Assessments: An Essential Tool for Data Protection* (presented at the Twenty-second Annual Meeting of Privacy and Data Protection Officials, 2000), online at http://aspe.os.dhhs.gov/datacncl/flaherty.htm (visited Jan 12, 2008) ("I conclude that the ideal privacy impact assessment of any project is prepared by someone from inside the project and with an up-front demonstration of just how it works or is supposed to work."); Blair Stewart, *Privacy Impact Assessment Towards a Better Informed Process for Evaluating Privacy Issues Arising from New Technologies*, 5 Privacy L & Policy Rep 147 (1999) ("PIA needs to be integrated into decision-making processes. For a government proposal, PIA might be integrated into departmental decision-making and appropriate cabinet processes. The important thing is that PIA not be divorced from decision-making processes.").

centralized decisionmaking, moreover, further supports this claim,[112] as do studies of cognition and decisionmaking, which emphasize "interaction with others whose thought processes are not governed by the same culture or knowledge structures as the decision maker" as a principal means of forcing integration of secondary concerns in tension with an organization's existing focus.[113]

Kelly's personnel decisions, then, reflected an attempt to break down traditional boundaries, both disciplinary and institutional. Particularly, as here, where the secondary mandate requires expertise outside the realm of agency culture, the introduction of specialized personnel—a privacy infrastructure—is a necessary prerequisite for success. PIAs, a form of technology assessment[114] first pioneered in New Zealand and Canada in the mid-1990s,[115] seek to elicit risks that cannot be identified through a legal lens alone, but also implicate "moral[,] ethical," and policy tradeoffs in technology design choices.[116] As such, they have been lauded for moving privacy decisions from a bureaucratic framework of compliance with "fair information practices," to deeper risk analyses and broader engagement of diverse constituents

---

112 W. Richard Scott, *Organizations: Rational, Natural and Open Systems* 262–63 (Prentice Hall 4th ed 1998) (discussing scholarship suggesting that centralization and formalization may be viewed as alternative control mechanisms: more formalized arrangements permit more decentralized decisionmaking).

113 Bamberger, 56 Duke L J at 443 (cited in note 38), citing Chip Heath, Richard P. Larrick, and Joshua Klayman, *Cognitive Repairs: How Organizational Practices Can Compensate for Individual Shortcomings*, 20 Rsrch Org Beh 1, 20 (1998) ("Often, organizations ensure that individuals weigh information effectively by forcing them to interact with others who might weigh the information differently."); James P. Walsh, *Managerial and Organizational Cognition: Notes from a Trip Down Memory Lane*, 6 Org Sci 280, 291 (1995) ("[R]esearch on the process of knowledge structure development suggests that a dramatically altered information environment is often the locus of knowledge structure change.").

114 Technology assessments aim to provide a framework for identifying and exploring the potential implications of different technological and system choices within and during technological development. Technology assessments are part of the broader research on the social shaping of technology (SST), which aims to view technology as sites of social interaction, politics, and power. A primary goal of the discipline is to demystify and democratize decisions about technology and to subject them, like other forms of power, to social accountability and control. PIAs that introduce other values into the conversation about technology selection, design, and deployment are a specific manifestation of this work. For a brief overview of the SST literature, see generally Robin Williams and David Edge, *The Social Shaping of Technology*, 25 Rsrch Policy 865 (1996).

115 See generally Stewart, 5 Privacy L & Policy Rep 147 (cited in note 111) (noting that PIAs have been implemented in jurisdictions of New Zealand since the early 1990s); Office of the Privacy Commissioner of Canada, *Fact Sheet: Privacy Impact Assessments* (2003), online at http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp (visited Jan 12, 2008) (detailing principles and procedures for conducting PIAs in Canada).

116 Flaherty, *Privacy Impact* (cited in note 111) (describing the interaction between privacy advocates and data collection system designers as cooperative and necessary for improved comprehension).

in a privacy dialogue. Optimal use of this new tool required the interdisciplinary staff assembled in the DHS privacy office.

3. Creating accountability in the absence of oversight: the Data Privacy and Integrity Advisory Committee.

Finally, the US-VISIT process was conducted in the context of a third important factor unique to DHS: the establishment of DPIAC, a federal advisory committee created in 2004 to oversee DHS privacy activities.[117] The enhanced accountability made possible through the creation of this external quasi-oversight board strengthened and publicized DHS privacy office processes and substantive decisions, thus enabling the office to further its subgoal within the agency.

Faced with a relative void in external oversight mechanisms geared to ensure compliance with privacy directives and the need to strengthen privacy's position within the conflicting DHS missions, Kelly requested Secretary Ridge's support to establish the DPIAC early on. She credits him with understanding that the creation of a "structure for consistent oversight by privacy and security experts" was essential for the office and the agency as a whole to both establish credibility and formalize the conversation about "what is a reasonable amount of government data collection even in the most extreme circumstances."[118]

The Committee, which met quarterly and set its own agenda, was comprised of privacy and security experts from the public and private sectors with sophisticated knowledge of technology and privacy. With the exception of one individual, none of the members fall into the category of privacy "advocates." Rather, they were respected individuals within corporate America and academia with sound privacy and security credentials.[119] Their ties to industry, the defense sector, and academia gave them particular force when they spoke to a privacy or security issue.

The DPIAC created a consistent form of oversight, pulling DHS officials from various departmental units to discuss privacy and security issues within specific projects. Importantly, the ability of the DPIAC to engage in a rather freewheeling review of DHS activity

---

117 See DHS Privacy Office, *Data Integrity, Privacy, and Interoperability Advisory Committee*, 69 Fed Reg 18923, 18923 (2004).

118 Kelly Interview (cited in note 95).

119 See DHS, *Department of Homeland Security Announces Appointments to Data Privacy and Integrity Advisory Committee* (Feb 23, 2005), online at http://www.dhs.gov/xnews/releases/press_release_0625.shtm (visited Jan 12, 2008) (listing initial appointees and noting that "members of this Advisory Committee have diverse expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the non-profit sector ... [and] also reflect a depth of knowledge on issues of data protection, openness, technology, and national security").

introduced an external expert quasi-oversight body to whom agency personnel, including those within operational divisions, had to account for their actions and decisions. Research into the psychology of accountability indicates the benefits of this type of review, in which decisionmakers are required to explain themselves to others whose views they do not know in advance.[120] In particular, such accountability "motivates" people "to anticipate the counterarguments that potential critics could raise to their positions."[121] It develops tolerance for cognitive inconsistency, so that a decisionmaker recognizes good features of rejected policies and bad features of accepted policies. It fosters a greater awareness of the cognitive processes underlying the decision. Finally, it counters the reliance on "existing knowledge structures in interpreting new information," making decisionmakers more willing to revise initial impressions of the situation in response to changing evidence.[122]

DRAWING CONCLUSIONS

Drawing on certain structures established by statute, internal high-level agency support, and an approach to personnel and expertise drawn from professional experience, the DHS CPO was able to manufacture the conditions for meaningful privacy impact assessment implementation in the absence of external oversight. Subsequent events within DHS combine with the differential cross-agency PIA performance, however, to underscore the contingency of such an outcome. Structurally, on his appointment, new DHS Secretary Michael Chertoff created an office for central oversight of agency policy, including privacy, drawing authority away from the separate privacy office.[123] Operationally, after a ten-month vacancy following Kelly's resignation, the CPO post was filled with Hugo Teufel III, a less-activist proponent of his office's authority who had little expertise with privacy policy beyond Privacy Act notices and FOIA requests, and weak ties with the privacy profession outside government.[124]

---

120 See, for example, Philip E. Tetlock, *Accountability: The Neglected Social Context of Judgment and Choice*, in Barry M. Staw and L.L. Cummings, eds, 7 Rsrch Org Beh 297, 314–21 (1985) (reviewing research on heuristics and stating that accountability can cultivate sensitivity to complex thinking practices under certain circumstances).

121 Id at 314, 316.

122 Id.

123 DHS also appointed Stewart Baker to the agency's lead policy position. Baker was formerly general counsel to the National Security Agency and a longtime and powerful influence for flexibility in government power. See DHS, *Assistant Secretary for Policy: Stewart A. Baker*, online at http://www.dhs.gov/xabout/structure/biography_0135.shtm (visited Jan 12, 2008).

124 See Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight after 9-11* 15 (SSRN Working Paper Series, 2006), online at http://pa-

In this light, our preliminary analysis suggests several factors that are worth further examination as means to institutionalize meaningful PIA compliance so as to reduce discretion and instability across context and time: (1) the independence of privacy decisionmakers within the agency structure; (2) external oversight largely unfettered by political and technical barriers; and (3) the incorporation of multiperspective analysis throughout decisions about information technology.

The statutory measures Congress successfully uses to control, ex ante, the exercise of bureaucratic discretion and overcome shortcomings of ex post oversight[125] seem particularly well suited to creating structures that institutionalize the independence of the agency privacy function. In particular, the RFID experience suggests the importance of reporting both directly to the agency head in order to preserve status as against other agency subunits, and to Congress, enhancing autonomy from both the agency and the executive branch more broadly by creating a means of dotted-line access to legislative, public, and press oversight on the inclusion of secondary mandates like privacy, which may encounter systemic resistance by the primary substantive goals around which agencies are otherwise organized. One such proposal before Congress dealing specifically with the DHS CPO—the Privacy Officer with Enhanced Rights Act of 2007[126]—would create these statutory safeguards, as well as privacy office investigatory power to access all agency documents and subpoena private sector materials and agency reporting requirements if the privacy officer is transferred or removed from office.

The PIA experience's lessons about the importance of, and barriers to, external oversight further resonate with a corpus of work by privacy scholars and professionals advocating the establishment of an independent agency to oversee the development and implementation of privacy policy.[127] While these general lessons do not speak to the

---

pers.ssrn.com/sol3/papers.cfm?abstract_id=933690 (visited Jan 12, 2008) (discussing the controversy over Teufel's appointment).

125 See McCubbins, Noll, and Weingast, 75 Va L Rev at 481 (cited in note 52) (emphasizing the opportunities to control bureaucracies through ex ante regulation); Barry R. Weingast and Mark J. Moran, *Bureaucratic Discretion or Congressional Control? Regulatory Policymaking by the Federal Trade Commission*, 91 J Polit Econ 765, 780–92 (1983) (providing empirical evidence demonstrating that Congress can control regulatory policymaking without active monitoring).

126 S 332, 110th Cong, 1st Sess (Jan 18, 2007) (proposing to amend the Homeland Security Act of 2002 to clarify the investigative authorities of the privacy officer of the Department of Homeland Security).

127 See, for example, Simitis, 135 U Pa L Rev at 742–43 (cited in note 53) ("Efficient regulation presupposes the establishment of an independent control authority."); Flaherty, *Protecting Privacy in Surveillance Societies* at 381 (cited in note 102) (declaring that the most important finding of a five-country privacy study is that "an agency charged with implementation is essential to make the law work in practice").

comparative merits of various iterations proposed,[128] they do suggest the importance of external accountability as a means for strengthening the hand of privacy officers internally, the role of connections with the privacy profession for enhancing the legitimacy and effectiveness of an oversight institution, and the need for substantive technical expertise in the review of privacy and technology decisions. While such an independent oversight entity might, as in the case of the Council on Environmental Quality's NEPA oversight,[129] arise from executive branch initiative, the problems of changing presidential commitment and the incongruity between individual congressional committee jurisdictions and cross-agency privacy directives experienced in the PIA analysis suggest codification in statute both as a commitment measure and as a means for rationalizing oversight.

Finally, the RFID cases suggest the importance of staffing capacity and structure around privacy and, in particular, integrating privacy expertise in both centralized and distributed form into policymaking. More specifically, it suggests the role of interdisciplinary teams in privacy impact assessments and the need for both a central, high-status privacy office and the embedding of individuals charged with seeing through a privacy lens throughout agency subunits.

These final suggestions underscore the limits of formal law in operationalizing privacy; the successful integration of privacy concerns into agency decisionmaking poses, at least in part, a challenge of management—of personnel, structures, and processes. They also reflect, it must be noted, some tension in the broader-brush implications we have drawn from the PIA and RFID experience. Enhancing privacy function independence, for example, is inherently in tension with both integrating that function within teams and units, and increasing its status by creating direct agency-head reporting. Strong monitoring mindsets, moreover, tend to cancel out more cooperative impulses towards coordination between disciplines and units.[130] Yet, at a minimum, these preliminary indicators of barriers and aids to accountability strongly recommend the promise of broader qualitative and context-dependent analysis of efforts, from within and without administrative agencies, to implement privacy and technology policy specifically, and integrate secondary goals in agency decisionmaking more generally.

---

128 Compare Gellman, 54 Hastings L J at 1215–19 (cited in note 102) (calling for a nonregulatory, independent federal privacy board for promoting "Fair Information Practices" in the public and private sectors), with Letter from Center for Democracy & Technology (cited in note 102) (advocating for an Office of Privacy and Technology Assessment with broad powers).

129 See text accompanying notes 40–47.

130 See Donald C. Langevoort, *Monitoring: The Behavioral Economics of Corporate Compliance with Law*, 2002 Colum Bus L Rev 71, 96 (2002).