Volume VI - Article 6

THE NATIONAL COUNTERTERRORISM CENTER: FOREIGN AND DOMESTIC INTELLIGENCE FUSION AND THE POTENTIAL THREAT TO PRIVACY

The Honorable Bennie G. Thompson[*]

Spring 2006

Late last year, Americans woke, dressed, read the newspaper, and learned that the Federal Government had been spying on them for over three years. The White House had asked the *New York Times* not to publish an article detailing President Bush's authorization of National Security Agency (NSA) wiretapping of American citizens.[1] The paper consequently delayed publication of the story for a year.[2] When the news finally broke, it ignited a firestorm of public controversy.

Months after the attacks of 9/11, President Bush ordered the NSA, the Defense Department's electronic and signals intelligence collection agency, to intercept and conduct wiretaps on Americans' international telephone calls and e-mail messages.[3] Some intelligence and national security law experts have concluded that the President's procedure sidestepped court orders otherwise required for government monitoring of domestic communications.[4]

---

[*] The Honorable Bennie G. Thompson has represented the Second District of Mississippi since 1993 and currently serves as the Ranking Member of the Committee on Homeland Security, U.S. House of Representatives. This article was written with Thomas M. Finan, Counsel and Coordinator, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Julie A. Edelstein, a second year law student at the University of Pennsylvania Law School, and Hank Greenberg, an intern with the House Committee on Homeland Security.

[1] James Risen and Eric Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say*, N.Y. TIMES, Dec. 15, 2005, http://www.nytimes.com/2005/12/15/politics/15cnd-program.html?ex=1141448400&en=936b902bbe592d97&ei=5070.

[2] *Id.*

[3] *Id.*

[4] Dan Eggen and Walter Pincus, *Campaign to Justify Spying Intensifies*, THE WASHINGTON POST, Jan. 24, 2006, at A04.

Critics have charged that the administration violated the Foreign Intelligence Surveillance Act (FISA) of 1978, which was designed to protect Americans' privacy by requiring warrants for government eavesdropping.[5] Some lawmakers have expressed concern about the reticence of the White House to brief Congress on the program.[6]

The Bush Administration has defended both the legality and the usefulness of the program. Since its disclosure, Attorney General Alberto Gonzales has argued that Congress' authorization of military force after the 9/11 attacks gave the President the requisite power.[7] According to President Bush and other Administration officials, the wiretaps have yielded valuable intelligence that would otherwise have not been available.[8]

White House assurances have failed to assuage concerns about infringements on Americans' privacy rights. In a February 2006 Senate Judiciary Committee hearing, Senator Dianne Feinstein told Attorney General Alberto Gonzales, "I can only believe – and this is my honest view – that this program is much bigger and much broader than you want anyone to know."[9] For some, revelations of intelligence agencies' spying on Americans recalls the Church Committee investigations of the 1970s, in which the CIA, FBI, and NSA were implicated in mail-opening, wiretapping, and other gross violations of U.S. citizens' right to privacy.[10]

The public's understandable anger in response to these events has profound implications for the federal government's homeland security efforts. If the government fails to maintain the traditional line of separation between domestic intelligence operations and foreign intelligence

---

[5] *Id.*
[6] David Morgan, *House Democrat Says White House Nixed NSA Briefing*, REUTERS NEWS, Feb. 21, 2006, *available at* http://news.yahoo.com/s/nm/20060222/pl_nm/security_nsa_dc (last visited Mar. 23, 2006).
[7] *See e.g.,* Eggen and Pincus, *supra* note 4; Carol D. Leonnig, *Report Rebuts Bush on Spying*, THE WASHINGTON POST, Jan. 7, 2006, at A01.
[8] Barton Gellman et al., *Surveillance Net Yields Few Suspects*, THE WASHINGTON POST, Feb. 5, 2006, at A01.
[9] Maura Reynolds, *Gonzales Defends Spying as 'Limited and Lawful'*, THE LOS ANGELES TIMES, Feb. 7, 2006, at A-1.
[10] John Diamond, *NSA's Surveillance of Citizens Echoes 1970s Controversy*, USA TODAY, Dec. 18, 2005, *available at* http://www.usatoday.com/news/washington/2005-12-18-nsa-70s_x.htm.

operations, long-established privacy protections enshrined not only in the Constitution, but also in the guidelines, rules, and regulations that govern our domestic law enforcement agencies will be at risk. The American people will come to distrust a government bent on winning the war on terror at all costs, even if it means sacrificing their personal privacy.

One place where this breakdown of privacy protections could also occur is the National Counterterrorism Center (NCTC), initially a creation of the Bush Administration and now one of several new entities established in the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act).[11] The NCTC combines the intelligence capabilities of the CIA, the FBI, and other agencies in order to integrate and analyze intelligence information for the purpose of developing strategic plans to protect the homeland.[12] While the NCTC's mission should be encouraged, its constituent members have traditionally had very different missions and have operated under vastly different legal regimes. In the NCTC's zeal to help root out terrorists and their plans, it is possible that the rules of foreign intelligence gathering, which are largely free of civil liberties concerns, will overtake traditional rules that apply to both domestic intelligence and law enforcement operations. Given the risk of "mission creep," Congressional oversight alone will not ensure that the NCTC will adequately respect privacy rights.[13] Congress instead must empower the Privacy and Civil Liberties Oversight Board (PCLOB), a separate creation of the Intelligence Reform Act, to take an assertive role in this area.[14] Using the Department of Homeland Security's Privacy Office (DHS Privacy Office) as a model, Congress must provide the PCLOB with greater independence, increased oversight powers, and appropriate authority to

[11] Exec. Order No. 13,354, 3 C.F.R. 214 (2005); Intelligence Reform and Terrorism Prevention Act of 2004 § 1021, *reprinted in* 50 U.S.C.A. § 404o (2005) [hereinafter Intelligence Reform Act].
[12] Intelligence Reform Act § 1021.
[13] Todd M. Masse, THE NATIONAL COUNTERTERRORISM CENTER: IMPLEMENTATION CHALLENGES AND ISSUES FOR CONGRESS 10 (2005), http://www.fas.org/sgp/crs/intel/RL32816.pdf.
[14] Intelligence Reform Act, 5 U.S.C.A. § 601 note (West Supp. 2005) (Privacy and Civil Liberties Oversight Board).

guide the development of comprehensive, consistent, and effective privacy policies that will ensure that the NCTC becomes an effective means to protect our nation from terrorism – and not a tool to rob Americans of their rights.

The Department of Homeland Security Privacy Officer and Privacy Office

In the wake of 9/11, many Americans became concerned that sweeping new law enforcement powers adopted to bolster national security, to increase information sharing between the CIA and FBI, and to create a new department to address terrorist threats might render privacy rights a casualty of the war on terror. Without a plan for safeguarding privacy, "concerns [were] expressed on a bipartisan basis about the anticipated agency's ability to collect, manage, share, and secure personally identifiable information."[15] To alleviate this fear, Congress included a provision in the Homeland Security Act of 2002 (hereinafter "Homeland Security Act") that created within the DHS the first statutorily required Privacy Officer, an official who would be tasked with avoiding undue encroachment upon privacy rights.[16] The DHS Privacy Officer's responsibilities include: (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information; (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974; (3) evaluating legislative and regulatory proposals involving collection, use and disclosure of personal information by the federal government; (4) conducting privacy impact assessments of proposed DHS rules on the privacy of personal information, including the type of personal information collected and the number of people affected; and (5) preparing a report to Congress

[15] *Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security: Hearing Before the Subcomm. on Commercial & Admin. Law of the House Comm. on the Judiciary*, 108th Cong. 28 (2004) [hereinafter *Hearings*] (statement of Chris Cannon, Chairman of the Subcomm. on Commercial and Admin. Law).
[16] Homeland Security Act § 222, 6 U.S.C.A. § 142 (West Supp. 2005).

on an annual basis about DHS activities that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.[17] "The establishment of [the DHS Privacy Officer position] is consistent with the DHS' fundamental responsibility to improve security while protecting the civil liberties of all Americans," noted Michael Scardaville of the Heritage Foundation shortly after the Act's passage.[18] "As the DHS develops ways to prepare for and predict terrorist threats," he added, "it is also important that it not overreach and either infringe on civil liberties or lay the groundwork on which a future administration might restrict freedom."[19]

The creation of the DHS Privacy Officer position was a watershed – first and foremost because of its uniqueness. For years, a number of federal agencies had "Privacy Act officers," but those individuals were often mid-level career officials who had no power to influence policymaking.[20] Moreover, although the Clinton Administration had required agencies to "designate a senior official . . . to assume primary responsibility for privacy policy," many such officials were political appointees who left their posts in 2001 with the change in administrations.[21] None of the positions were statutorily created, and none were guaranteed to exist in perpetuity. By contrast, the DHS Privacy Officer position is a creature of statute – a development that not only ensures its permanency within the DHS but also subjects it to congressional review.[22] This arrangement accordingly promotes greater accountability and

---

[17] *Id.*
[18] Michael Scardaville, *Principles the Department of Homeland Security Must Follow for an Effective Transition*, The Heritage Foundation (Feb. 28, 2003), http://www.heritage.org/Research/HomelandDefense/bg1630.cfm.
[19] *Id.*
[20] *Hearings*, *supra* note 15, at 66 (testimony of James Dempsey, Executive Director of the Center for Democracy and Technology).
[21] *Id*. at 67.
[22] *Id.* at 7 (statement of Chris Cannon, Chairman, Subcomm. On Commercial & Admin. Law).

adherence to privacy laws.[23] To this day, the DHS Privacy Officer position is the only such statutory position in the Federal Government.[24]

The DHS Privacy Officer is supported by the DHS Privacy Office, which works to promote best practices and to otherwise "operationalize" privacy throughout the DHS culture.[25] Toward that end, the first DHS Privacy Officer, Nuala O'Connor Kelly, summarized her Office's role as being "not only to inform, educate, and lead privacy practice within the Department, but also to serve as listeners and as a receptive audience to those outside the Department who have questions or concerns about the Department's operations."[26] In so doing, the DHS Privacy Office operates as a "helpmate" to pre-empt and prevent privacy abuses.[27] The DHS Privacy Office is especially important, however, because of its power to substantively affect policy within the DHS.[28] As O'Connor Kelly described:

> Through internal educational outreach and the establishment of internal clearance procedures and milestones for program development, we are helping DHS components to consider privacy whenever developing new programs or revising existing ones. We are evaluating the use of new technologies to ensure that privacy protections are given primary consideration in the development and implementation of these new systems. In this process, DHS professionals have become educated about the need to consider – and the framework for considering – the privacy impact of their technology decisions. We are reviewing Privacy Act systems notices before they are sent forward and ensuring that we collect only those records that are necessary to support our mission. We also guide DHS agencies in developing appropriate privacy policies for their programs and serve as a resource for any questions that may arise concerning privacy, information collection or disclosure. And the Privacy Office of course works closely with various DHS policy

[23] *See e.g.* Steve Lilenthal, *Wanted: Privacy Officer By Statute, Not Discretion*, Free Congress Foundation, Feb. 13, 2004, http://www.freecongress.org/commentaries/040213sl.asp.
[24] *Hearings*, *supra* note 15 at 65 (statement of James Dempsey, Executive Director of the Center for Democracy & Technology).
[25] *Id.* at 25 (testimony of Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Dep't of Homeland Sec.).
[26] *Id.* at 27.
[27] Sarah Lai Stirland, *Panel Queries Officials About Intelligence Oversight, Privacy* (Aug. 20, 2004), GOVEXEC.COM, *available at* http://www.govexec.com/dailyfed/0804/082004tdpm2.htm.
[28] Lorraine Carlson, *Nuala O'Connor Kelly: Privacy Officer to the Nation*, TRUSTe, *available at* http://truste.org/articles/dhsprivacyofficer.php (last visited Feb. 3, 2006).

teams, the Office of the General Counsel, and the Chief Information Officers to ensure that the mission of the Privacy Office is reflected in all DHS initiatives.[29]

In short, the DHS Privacy Office is responsible not only for oversight of privacy matters but also for helping to develop consistent, comprehensive, and effective guidelines for protecting privacy throughout the twenty-two legacy agencies that comprise the DHS.[30] The Office's means of accomplishing its goals is multi-layered; in addition to issuing systems of records notices, general privacy orders, and privacy memos, it influences policy through its Privacy Impact Assessments (PIA's).[31] PIA's analyze the privacy impact of any substantially revised or new "Information Technology System," as mandated by the E-Government Act of 2002.[32] The DHS Privacy Office already has released numerous PIA's on significant policy initiatives, including US-VISIT (which is being designed to capture entry and exit information from non-immigrant visa holders) and Secure Flight (a proposed passenger pre-screening system for commercial aviation).[33]

Despite these impressive efforts and successes, neither the DHS Privacy Officer position nor the DHS Privacy Office are perfect answers to the question of how to preserve privacy rights in the post-9/11 world. On the contrary, the DHS Privacy Officer needs greater independence and adequate authority in order to properly evaluate privacy concerns within the DHS – without regard to political pressures. That is a level of independence that simply has not been granted to date. Accordingly, a dozen members of Congress have sponsored H.R. 3041, the Privacy Officer with Enhanced Rights (POWER Act) to address these shortcomings.

---

[29] *Hearings*, *supra* note 15 at 19 (testimony of Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Dep't of Homeland Sec.).
[30] Carlson, *supra* note 28.
[31] Department of Homeland Security, *Privacy Office – Privacy Impact Assessments (PIA)*, http://www.dhs.gov/dhspublic/interapp/editorial_0511.xml (last visited Feb. 3, 2006).
[32] Department of Homeland Security, *The Privacy Office of the U.S. Department of Homeland Security*, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0338.xml (last visited Feb. 3, 2006).
[33] Department of Homeland Security, *supra* note 31.

The POWER Act would provide the DHS Privacy Officer with the authority to require DHS employees to produce documents and to answer questions relevant to privacy matters, a power currently enjoyed by the DHS Inspector General. In addition, it would establish a set term for the DHS Privacy Officer and also require her to submit privacy reports directly to Congress – without any prior comment or amendment from the DHS Secretary. "The POWER Act will help to ensure that the accountability necessary to determine if DHS agencies are adequately protecting privacy and following current law and policy," said Ari Schwartz of the Center for Democracy and Technology.[34] Indeed, an independent and effective DHS Privacy Officer is precisely what the Department needs to guard against the kinds of abuses recently reported with the NSA's domestic spying program. "We understand that a truly vigorous and independent privacy officer can be inconvenient for government officials over the short term," ACLU attorney Tim Sparapani has noted.[35] "But over the long run, vigorous checks and balances will strengthen the Department of Homeland Security by inspiring greater public confidence in DHS programs . . ."[36]

Even if the POWER Act fails to become law, however, the DHS experience can and should serve as a template for preserving privacy throughout the executive branch. As James X. Dempsey of the Center for Democracy and Technology has noted, "[T]he DHS Privacy Officer legislation is a model for other agencies . . . With some further reforms we support . . . statutory Privacy Officers should be an important element of the overall approach to meeting the public's

[34] Letter from Ari Schwartz, Deputy Director, *Center for Democracy and Technology*, to Congressman Bennie G. Thompson (June 22, 2005) (on file with author).
[35] Ryan Singel, *Privacy Czarina Resigns*, Secondary Screening, Sept. 28, 2005, http://www.secondaryscreening.net/static/archives/2005/09/privacy_czarina.html.
[36] *Id.*

deeply-held and constitutionally-based interests in privacy protection even in the pursuit of urgent governmental missions like counterterrorism."[37]

Intelligence Analysis and Integration: Missed Opportunities for Privacy Oversight

Congress' original plan to locate a collaborative intelligence analysis and integration center within the DHS would have placed that function squarely under the supervision of the DHS Privacy Office. Specifically, the Homeland Security Act created the Information Analysis and Infrastructure Protection Directorate (IAIP) to collect, analyze, and disseminate intelligence information about terrorist threats to the nation.[38] In early 2003, however, just months after the IAIP's creation, the Bush Administration began wresting that function from the DHS by creating a separate entity under the Director of Central Intelligence: the Terrorist Threat Integration Center (TTIC).[39] The TTIC, staffed by representatives on assignment from the CIA, the FBI, the DHS, and other agencies, inherited many of the analysis responsibilities of the IAIP before it even got off the ground.[40] Nevertheless, the TTIC's lifespan, like the IAIP's, was a short one.

In order to promote effective intelligence analysis, integration and information sharing,

---

[37] *Hearings*, *supra* note 15, at 64 (testimony of James Dempsey, Executive Director of the Center for Democracy & Technology).

[38] Homeland Security Act, 6 U.S.C.A. § 121 (West Supp. 2005).

[39] Press Release, The White House, Fact Sheet: Strengthening Intelligence to Better Protect America (Jan. 28, 2003) *available at* http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html; *See also* CLARK K. ERVIN, U.S. DEP'T OF HOMELAND SEC., DHS CHALLENGES IN CONSOLIDATING TERRORIST WATCH LIST INFORMATION (2004) (describing reasons why DHS was unprepared to take on intelligence fusion role anticipated by Congress).

[40] *See* James J. Carafano & David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, The Heritage Foundation and the Center for Strategic and International Studies, *at* http://www.csis.org.hs/041213_dhsv2.pdf (Dec. 13, 2004); Justin Rood, *A Curtain Comes Down on Homeland's Key Role in Counterterror Analysis,* 15, *at* http://page15.com/2004/10/curtain-comes-down-on-homelands-key.html (Oct. 12, 2004); Justin Rood, *Analysis: New Counterterror Center Proposals Make DHS Intel Efforts 'Irrelevant',* 15, *at* http://page15.com/2004/09/analysis-new-counterterror-center.html (Sept. 30, 2004); Seth G. Jones, *Terrorism and the Battle for Homeland Security*, Foreign Policy Research Institute, *at* http://www.fpri.org/enotes/20040521.americawar.jones.terrorismdhs.html (May 21, 2004); Michael Crowley, *Bush's Disastrous Homeland Security Department*, THE NEW REPUBLIC, Mar. 15, 2004; MARKLE FOUND., CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY, SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE 2 (2003).

the 9/11 Commission specifically recommended the creation of the NCTC, built on the foundation of the TTIC, to break "the mold of national government organization" by being "a center for joint operational planning *and* joint intelligence, staffed by personnel from the various agencies."[41] President Bush ultimately adopted the 9/11 Commission's recommendation in this regard and directed that the TTIC be integrated into the NCTC.[42] The NCTC's proposed mission, "encompasses IAIP's original analysis role, as set down in the Homeland Security Act of 2002 . . . which said the directorate should 'access, receive and analyze law enforcement information, intelligence information, and other information . . . and to integrate such information' to identify terrorist threats to the United States."[43] Then DHS Secretary Tom Ridge acknowledged as much in September 2004 during a hearing before the Senate Governmental Affairs Committee, when he testified that the NCTC would take over "a lot" of threat assessment responsibilities from the IAIP.[44] In response to the 9/11 Commission Report, and following the Bush Administration's creation of the NCTC by Executive Order, Congress formally established the NCTC as the primary fusion center for all terrorism intelligence analysis and integration in the Intelligence Reform Act in late 2004.[45]

By removing the intelligence analysis and integration function from the IAIP and the DHS, relocating it to the TTIC, and then finally moving it to the NCTC, the Bush Administration negated any constructive role that the DHS Privacy Office could have played in

---

[41] NATIONAL COMMISSION ON TERRORIST ACTS UPON THE UNITED STATES, THE 9-11 COMMISSION REPORT 403 (2004) [hereinafter THE 9-11 COMMISSION REPORT] (emphasis in original).
[42] Press Release, The White House, Reforming and Strengthening Intelligence Services (Sept. 8, 2004) *available at* http://www.fas.org/irp/news/2004/09/wh090804.html; Press Release, The White House, Making America Safer by Strengthening Our Intelligence Abilities (Aug. 2, 2004) *available at* http://www.fas.org/irp/news/2004/08/wh080204-fact.html.
[43] Rood, *Analysis: New Counterterror Center Proposals Make DHS Intel Efforts 'Irrelevant'*, *supra* note 40.
[44] DHS/IAIP DAILY REPORT TEAM, DAILY OPEN SOURCE INFRASTRUCTURE REPORT, 10 (Sept. 15, 2004), *available at* http://www.cargosecurity.com/ncsc/ncsc_dotnet/uploads/DHS_IAIP_Daily_2004-09-15.pdf; Dibya Sarkar, *DHS to Push Counterterror Info*, FED. COMPUTER WKLY., Sept. 13, 2004, http://www.fcw.com/fcw/articles/2004/0913/web-ridge-09-13-04.asp.
[45] Intelligence Reform Act, *supra* note 11.

"operationalizing" privacy into this critical component of the nation's counterterrorism arsenal. In fact, the DHS' privacy oversight opportunities were squandered as soon as the Bush Administration divested the IAIP of its responsibilities. As the Markle Foundation noted at that time:

> [T]he Executive Branch should create within the TTIC the appropriate institutional mechanisms to safeguard privacy rights. When Congress passed legislation to establish the DHS, it was careful to include a privacy officer and a civil rights and civil liberties officer. If the TTIC is going to perform much of the analysis and information–sharing mission Congress had intended for the DHS, then it should have commensurate privacy-protection measures.[46]

The Bush Administration never effectively followed through – either with the TTIC or the NCTC – to fulfill the Homeland Security Act's explicit goal of bolstering privacy rights while strengthening our nation's post-9/11 intelligence capabilities. This is an unacceptable situation, especially with an entity like the NCTC, where agencies traditionally involved in foreign intelligence operations overseas are commingled with agencies responsible for domestic intelligence and law enforcement activities.

The CIA, the FBI, and the NCTC: A Recipe for Mission Creep

Intelligence reforms undertaken in the 1970s largely limited the CIA to gathering foreign intelligence abroad while providing the FBI with domestic law enforcement and intelligence responsibilities, specifically for counter-espionage and international terrorism investigations.[47] Kate Martin, Director of the Center for National Security Studies, described the importance of this dichotomy for civil liberties purposes:

> The CIA acts overseas, in secret, and its mission includes violating the laws of the country in which it is operating when necessary. It is charged with collecting information overseas without regard to individual privacy, rights against self-incrimination, or requirements for admissibility of evidence. It is also tasked with carrying out covert actions to influence events by whatever means the President authorizes. The agency

[46] Markle Foundation, *supra* note 40, at 19.
[47] Kate Martin, *Domestic Intelligence and Civil Liberties*, SAIS REV., Winter-Spring 2004, at 10.

> gives the highest priority to protection of its sources and methods. In contrast, the FBI's law enforcement efforts involve the collection of information for use as evidence at trial, and its methods and informants are quite likely to be publicly identified. Perhaps most significantly, law enforcement agencies, unlike intelligence agencies, must *always* operate within the law of whatever jurisdiction in which they are operating.[48]

Although the National Security Act of 1947, which created the CIA, prohibits the CIA from exercising "police, subpoena, or law enforcement powers or internal security functions," it is still permitted to conduct intelligence operations against Americans inside the United States so long as the CIA's purpose is not, among other things, to acquire information concerning their "domestic activities."[49] Moreover, Executive Order 12333 requires that "[t]he collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General."[50] Addressing these restrictions, Martin further noted key differences between government investigations for foreign intelligence purposes and investigations for law enforcement purposes:

> The constitutional concerns for Fourth Amendment due process and First Amendment rights of Americans and others located inside U.S. borders do not extend to aliens overseas and thus place fewer restrictions on government activity abroad than at home. (An intelligence agency collecting information overseas for use by policymakers has less opportunity to improperly use that information against individuals than does a police agency working with prosecutors.) While the task of foreign intelligence is to learn as much as possible to provide analyses to policymakers, deep-seated notions of privacy

---

[48] *Id.* (emphasis in original).

[49] Center for National Security Studies, *Intelligence Activities in the United States: Recommendations to Protect Civil Liberties* 6 (2005), *available at* http://www.cnss.org/domintel%200305.doc (*citing* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *as amended by* Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Sept. 1, 2004) [hereinafter Exec. Order No. 12,333]). The CIA is also authorized to collect and keep broad categories of information including: publicly available information, information obtained in the course of lawful foreign intelligence, counterintelligence or counterterrorism investigation, and information about Americans "reasonably believed to be potential sources or contacts." Exec. Order No. 12,333, §§ 2.3(a), (c), and (f)); *see also* Richard A. Best, Jr. et al., *Director of National Intelligence: Statutory Authorities*, Congressional Research Service, 2-3 (April 8, 2005) *available at* http://www.fas.org/sgp/crs/intel/RS22112.pdf (noting that the Intelligence Reform Act restates the major responsibilities of the CIA Director, which include the collection of intelligence through human sources and by other appropriate means, "but with no police, subpoena, or law enforcement powers or internal security functions ….").

[50] Exec. Order No. 12,333, § 1.8(a).

> rooted in the Constitution limit the information the government may collect and keep about Americans.[51]

Observers have long recognized the risks to civil liberties presented by the expanding missions and roles of domestic intelligence agencies, missions that at the NCTC now include the sharing of foreign and domestic intelligence by the CIA, the FBI, and other agencies. More than five years before 9/11, Stewart Baker, the former general counsel of the National Security Agency, commented that "[i]ntelligence-gathering tolerates a degree of intrusiveness, harshness, and deceit that Americans do not want applied against themselves."[52] "Combining domestic and foreign intelligence functions," he warned, "creates the possibility that domestic law enforcement will be infected by the secrecy, deception, and ruthlessness that international espionage requires."[53] While Baker concluded that the Department of Justice (DOJ) has served as an effective check on intelligence activities in the United States since reforms were adopted in the 1970s, he opined, in a particularly prescient comment, that "should it [DOJ] come to depend on the intelligence agencies to help it enforce the law, the department will be less credible, and perhaps less vigilant, as a guardian of civil liberties."[54]

Stephen Marrin, a former analyst with both the CIA and the General Accounting Office's Defense Capabilities and Management Team, has since documented the apparent realization of this fear:

> The ability to use counterterrorism surveillance capabilities for general law enforcement purposes will be a temptation not easily resisted, and such mission expansion may already be occurring. In February 2003, the *New York Times* reported that "FBI-led task forces whose primary duty is stopping al-Qaida and other international groups . . . have thwarted several would-be domestic terrorists in recent months," including specific plans by members of the Ku Klux Klan and Jewish militants. The article quoted U.S. Attorney Mary Beth Buchanan, who justified this expansion of focus by saying, "Domestic

[51] Martin, *supra* note 47, at 10.
[52] Stewart A. Baker, *Should Spies Be Cops?*, 97 FOREIGN POLICY, Winter 1994-95, at 40.
[53] *Id.* at 36-37.
[54] *Id.* at 40-41.

> terrorism can be devastating as well. We are continuing to deal with both." . . . By expanding the definition of "security threat" to encompass foreign individuals acting as lone-wolf terrorists and other domestic terrorist groups – including neo-Nazi groups, anarchic environmentalists, and animal liberation groups, it is only a small leap to apply counterterrorism capabilities to track and catch individual lawbreakers and everyday criminals."[55]

Under such circumstances, Marrin noted, "[d]omestic intelligence mission creep is highly likely due to the benefits accruing from other uses of the information."[56] He concluded that this threat can be countered by incorporating overlapping procedural guidelines and oversight mechanisms at the start of any new domestic intelligence program,[57] something apparently absent or otherwise ignored during the NSA's latest surveillance effort.[58]

Others have also warned about the mission creep danger. Prior to TTIC's integration into the NCTC, Bobby Brady, deputy chief information officer for the CIA, addressed the problem of information sharing between the CIA and the FBI in precisely these terms. "Our job is to develop intelligence on foreign threats and at the same time protect our data and sources," he said.[59] "[The] FBI has the task of domestic law enforcement and turning investigations into convictions. There is a reason we don't mix. [If we shared all information,] there would be legal and political ramifications we can't even foresee."[60] The Markle Foundation concurred:

> [T]he creation of the TTIC as an all-source intelligence fusion and analysis center—with access to both foreign intelligence and domestic intelligence and law enforcement information concerning U.S. persons—confronts us with the question of what will replace the previous "line at the border" that largely defined the distinctive rules for foreign and domestic intelligence. There has been no significant public debate on this fundamental question, and it is a critical area for presidential guidance. It is possible that

---

[55] Stephen Marrin, *Homeland Security Intelligence: Just the Beginning*, J. HOMELAND SEC., Nov. 2003, http://www.homelandsecurity.org/journal/Articles/marrin.html.
[56] *Id.*
[57] *Id.*
[58] Eggen and Pincus, *supra* note 4.
[59] Mathew French & Sara Michael, *CIA, FBI Wrangle Over Threat Center*, FEDERAL COMPUTER WEEKLY, (Apr. 28, 2003), *available at* http://www.fcw.com/article79474.
[60] *Id.*

> the Executive Branch has radically changed the balance of liberties with this organizational move.[61]

The same holds true for the NCTC. As Todd M. Masse noted shortly after its creation, "the possibility exists that unintentional mission creep and operational zeal could lead to situations in which rules designed to guide traditional foreign intelligence collection may be applied to U.S. persons."[62] He added that civil liberties could be at risk, "if domestic intelligence is directed against them in a manner that may not be consistent with or constrained by appropriate Attorney General Guidelines."[63] For example, a prolonged war on terror or the heightened threat posed by terrorists armed with a weapon of mass destruction might well lead some to ignore the Constitution, applicable statutes, and DOJ privacy and other regulations when (1) working with confidential informants; (2) performing undercover activities and operations; (3) using nonconsensual electronic surveillances, pen registers and trap and trace devices; (4) accessing stored wire and electronic communications and transactional records; (5) using consensual electronic monitoring; and (6) executing searches and seizures.[64]

Although the 9/11 Commission recommended that the NCTC should lead strategic analysis of all intelligence, foreign and domestic, pertaining to transnational terrorist organizations; should develop net assessments by comparing enemy capabilities and intentions against U.S. defenses and countermeasures; and should provide appropriate warnings to the public, it took heed of these concerns by recommending that the NCTC should *not* direct the actual execution of intelligence operations.[65] On the contrary, the 9/11 Commission made clear that the FBI, not the CIA, should be responsible for domestic intelligence responsibilities,

---

[61] Markle Foundation, *supra* note 40, at 18-19.
[62] Masse, *supra* note 13, at 10.
[63] *Id.*
[64] THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS (2002), http://www.usdoj.gov/olp/generalcrimes2.pdf at 6.
[65] THE 9-11 COMMISSION REPORT, *supra* note 41, at 404.

stating, "The FBI's job in the streets of the United States would thus be a domestic equivalent, operating under the U.S. Constitution and quite different laws and rules, to the job of the CIA's operations officers abroad."[66] This position found strong support among a bipartisan group of former high-ranking intelligence and national security officials, who during the debate over the Intelligence Reform Act argued:

> Even as we merge the domestic and foreign intelligence we collect, we should not merge responsibility for collecting it . . . exclusive responsibility for authorizing and overseeing the act of domestic intelligence collection should remain with the Attorney General. This is the only way to protect the rights of the American people upon whose support a strong intelligence community depends.[67]

Unfinished Business: the Privacy and Civil Liberties Oversight Board

The Intelligence Reform Act ushered in a complete reorganization of the Intelligence Community that included, among other things: (1) replacing the Director of Central Intelligence (DCI) with a Director of National Intelligence (DNI), who not only reports directly to the President on intelligence matters, but also serves above the head of the CIA; (2) formalizing the establishment of the NCTC as set forth in President Bush's Executive Order 13354; and (3) establishing the Privacy and Civil Liberties Oversight Board (PCLOB).[68] Congress created the PCLOB, presently located within the Executive Office of the President, in direct response to the 9/11 Commission's admonition that legislation should be crafted in order to promote, "an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."[69]

Unlike the DHS Privacy Office, however, the PCLOB has no mandate to inform, educate, or lead privacy practice among those executive branch components involved in war on terror-

[66] *Id.* at 423 (emphasis added).
[67] 150 CONG. REC. S9429 (daily ed. Sept. 21, 2004) (statement of Rep. Stevens).
[68] Intelligence Reform Act, *supra* note 11, §§ 1011, 1021, 1061.
[69] *Id*. at §1061; THE 9-11 COMMISSION REPORT, *supra* note 41, at 395

related intelligence and law enforcement activities. It likewise has no power to help develop consistent, comprehensive, and effective privacy guidelines within those components. Instead, the PCLOB can only "advise" the President and agency and department heads to ensure that privacy and civil liberties "are appropriately considered" and advise when adequate guidelines are lacking.[70] Unlike the DHS Privacy Office, moreover, the PCLOB has practically no independence from the White House. For example, the PCLOB consists of five members (1) all of whom are appointed by the President, and only two of whom, the chairman and vice-chairman, require Senate approval; (2) all of whom serve "at the pleasure of the President"; (3) none of whom need be of different political parties; and (4) none of whom need have any expertise in civil liberties matters.[71] The PCLOB's oversight ability, moreover, is severely constrained because it lacks the subpoena power.[72]

Compounding these problems, it was not until June 2005, six months after the Intelligence Reform Act was enacted, that President Bush actually nominated anyone to the PCLOB – nominations that he did not send on to the Senate until September 2005.[73] The Senate did not actually approve his chairman and vice chairman picks until February 2006.[74] Making matters worse, the President set aside only $750,000 for the PCLOB in his fiscal 2006 budget, a mere fraction of the $13 million allotted to the DHS Privacy Office.[75] While lawmakers subsequently doubled that amount during the appropriations process, the President's fiscal 2007

---

[70] Intelligence Reform Act §1061(c)(1)(C) & (D).
[71] *Id*. at §1061(e)(1).
[72] *Id*. at §1061(d).
[73] Brian Friel, *Civil Liberties Board Has Yet To Get Off the Ground* (Jan. 13, 2006), GOVEXEC.COM, *available at* http://www.govexec.com/story_page.cfm?articleid=33176&printerfriendlyVers=1&; Richard B. Schmitt, *Privacy Guardian Is Still a Paper Tiger*, THE LOS ANGELES TIMES, Feb. 20, 2006, *available at* http://www.latimes.com/news/nationworld/nation/la-na-liberties20feb20,0,5039697.story?coll=la-home-headlines.
[74] Schmitt, *supra* note 73.
[75] Eric Lichtblau, *Senators Say Bush Lags on Creating Terror Panel*, N.Y. TIMES, May 15, 2005, at 30, *available at* http:www.nytimes.com/2005/05/15/politics/15rights.html; Justin Rood, *White House Leaves Civil Liberties Board Unfunded, Unstaffed*, CQ-HOMELAND SECURITY – INTELLIGENCE, Apr. 4, 2005, *available at* http:homeland.cq.com/hs/display.do?docid=1599232&sourcetype=31&binderName=News-all.

budget includes no express funding for the PCLOB at all – an omission that has resulted in an outcry from both Democratic and Republican quarters.[76] "The failure to move on the [PCLOB] is part of a disturbing trend," one commentator stated last year.[77] "Too often, the Bush White House has chosen to simply ignore that which it doesn't like. Congress didn't vote to ask the administration to think about having a privacy board. It established the board and gave the White House the power to populate it."[78] Many other observers have similarly concluded that the PCLOB amounts to nothing more than a powerless entity that is unequipped to accomplish the goals laid out by the 9/11 Commission.[79]

To address these problems, a bipartisan group of members of the House of Representatives has sponsored the Protection of Civil Liberties Act, H.R. 1310.[80] The Act would address the litany of deficiencies with the PCLOB by (1) establishing it as an independent agency in the executive branch outside the Executive Office of the President; (2) requiring that all five of its appointed members be confirmed by the Senate; (3) requiring that no more than three of its members hail from the same political party; (4) setting six-year, staggered terms for the members; (5) requiring that members have prior experience with protecting civil liberties; (6) specifying that the chairman shall be a full-time member of the PCLOB; (7) increasing PCLOB's Congressional reporting requirement from once to at least twice yearly; and (8) requiring that each executive department or agency with law enforcement or antiterrorism functions designate a

---

[76] Schmitt, *supra* note 73; Tim Starks, *Bush Budget Leaves Out Money for Oversight of Privacy and Civil Liberties*, CQ TODAY, Feb. 7, 2006, *available at* http://www.cq.com/display.do?dockey=/cqonline/prod/data/docs/html/news/109/news109-000002046131.html@allnews&metapub=CQ-NEWS&searchIndex=1&seqNum=1.

[77] *Civil Liberties Board Has Got to Get Into Gear*, MASSLIVE.COM, May 17, 2005, http://www.masslive.com/editorials/republican/index.ssf?/base/news-0/1116316055289570.xml@coll=1.

[78] *Id.*

[79] *See* Lichtblau, *supra* note 75; Letter from ACLU to Representatives Carolyn Maloney, Tom Udall & Christopher Shays (March 15, 2005) (on file with author); Press Release, Voices of September 11th, *Giving Teeth to the Civil Liberties Board Recommended by the 9/11 Commission* (March 15, 2005), http://www.voicesofsept11.org/911ic/031505 (last visited Mar. 23, 2006).

[80] Protection of Civil Liberties Act, H.R. 1310, 109th Cong. (2005).

privacy and civil liberties officer.[81] Perhaps most importantly, the Act would give the PCLOB the subpoena power so it can conduct a meaningful analysis of privacy and other civil liberties protections.[82]

H.R. 1310 is an excellent start to preserving the privacy of all Americans as our nation fights the war on terror. Given the aforementioned risk of "mission creep," however, Congress should take several additional steps to specifically address the intelligence analysis and integration function being performed by the CIA, the FBI, and other agencies at the NCTC.

First, Congress should expand the PCLOB's mission beyond merely "advising" agency and department heads about privacy and civil liberties concerns to "reviewing" their policies, procedures, and regulations.[83] Using the DHS Privacy Office as a model, Congress should draft legislation designating the PCLOB as the gatekeeper for all existing or proposed policies, procedures, regulations, *and programs* by any executive branch components involved in war on terror-related intelligence activities. Specifically, Congress should require those components, including the CIA, the FBI, and all other NCTC constituent agencies, to proactively consult with the PCLOB before, during, and after implementation. In so doing, those components can "operationalize" privacy, both at the outset of any initiative and throughout its duration. To support this mission, Congress should also provide the PCLOB with the power to audit any policy, procedure, regulation, or program undertaken without prior input from the PCLOB so that Congress can be advised of any privacy concerns on an expedited basis.

In addition, Congress should provide the PCLOB with the authority to establish privacy "clearance" procedures and milestones that the NCTC and its constituent agencies must satisfy regarding the development of any new technology-based program used to assemble, analyze,

[81] *Id.* §§ 3-4,6.
[82] *Id.* §5.
[83] Intelligence Reform Act, § 1061.

integrate, and/or disseminate the personal information of American citizens. As part of that process, the PCLOB, like the DHS Privacy Office, should be empowered to evaluate technologies identified by those agencies through PIA's (as prescribed in the E-Government Act of 2002) in order to verify that appropriate privacy safeguards are incorporated before those technologies come on line.

Finally, Congress should authorize the PCLOB to issue general privacy guidelines and orders so the PCLOB can harmonize privacy policy at the NCTC. By doing so, Congress will guarantee for the PCLOB the same informational, educational, and leadership role among the NCTC's constituent agencies that the DHS Privacy Office presently enjoys among the twenty-two legacy agencies that comprise the DHS.

A coordinated privacy policy among these agencies would go a long way toward ensuring they all start on the same privacy "page," a need for which the NSA domestic spying program vividly demonstrates. Furthermore, a consistent approach in this area would create common experiences and understandings of privacy rights, not only within these agencies, but also among the American people. This would boost the institutional credibility of new entities like the NCTC by showing that the Federal Government is mindful of privacy issues and consequently would inspire confidence in the NCTC's mission.

Second, Congress should draft legislation that (1) delineates the legal authorities that govern each of the NCTC's constituent agencies, including the CIA and the FBI, regarding counterterrorism operations; and (2) provides the PCLOB with explicit oversight authority over the NCTC, especially when its operations involve Americans.[84] The Center for National Security Studies warns that the Intelligence Reform Act "removed some of the existing bureaucratic impediments to greater CIA domestic activities, while giving authority to the new

[84] Masse, *supra* note 13, at 10.

DNI or Director of the National Counterterrorism Center (NCTC) to task the CIA to carry out domestic intelligence activities, not even limited to collection activities."[85] The Center points specifically to Section 119 of the Act, which provides that the NCTC Director can task intelligence agencies with carrying out, "strategic operational plans . . . for [] counterterrorism efforts . . . *both inside and outside the United States*."[86] The Center concludes, "[i]t is not clear that the 1981 E.O. requirement [Executive Order 12333] that CIA activities inside the United States be coordinated with the FBI and conducted pursuant to guidelines approved by the Attorney General will survive these changes."[87] Masse addresses this same problem in reference to President Bush's more recent Executive Order 13354:

> It is explicitly stated in the executive order that ". . . each agency representative to the Center [NCTC], unless otherwise specified by the DCI, shall operate under the authorities of the representative's agency." That is, while strategic planning may be joint, if the NCTC Director assigns the FBI, CIA, and Department of Defense certain counterterrorism operations responsibilities, each agency operates under its own legal authorities. While it may be implicit, *no such similar and explicit legal authority guidance was provided in P.L. 108-458* [the Intelligence Reform Act].[88]

Without certainty in the law, there can be no accountability under the law – something the Bush Administration's current attempts to justify the NSA domestic surveillance program makes abundantly clear.[89] In order to promote public confidence in our homeland security efforts, Congress must amend the Intelligence Reform Act to clarify that when it comes to domestic intelligence operations, the CIA, the FBI, and others are bound not only by the Constitution, but also by the guidelines, rules, and regulations that have traditionally governed such activity.

---

[85] Memorandum from The Center for National Security Studies, *supra* note 49, at 6.
[86] *Id.* (citing Intelligence Reform Act §119(f)(1)(B), 50 U.S.C. §402 (2005) (emphasis added).
[87] *Id.*
[88] Masse, *supra* note 13, at 10. *See* Exec. Order No. 13,354, 69 Fed. Reg. 53,589 (Aug. 27, 2004) (emphasis added).
[89] *See e.g.,* Eggen and Pincus, *supra* note 4; Gellman, *supra* note 8.

With the Homeland Security Act's creation of the DHS Privacy Officer position, Congress initiated a commitment to preserving privacy rights throughout the war on terror. That commitment continued after the issuance of the 9/11 Commission Report, a report that not only informed Congress' efforts while drafting the Intelligence Reform Act but also emphasized the different roles played by the CIA and the FBI in foreign and domestic intelligence operations, respectively.[90] As noted previously, when urging that the NCTC should not be permitted to direct the actual execution of such operations, the 9/11 Commission drew a sharp distinction between CIA operations abroad, on the one hand, and domestic intelligence operations on the other.[91] To the extent some nevertheless might use the NCTC as a means to introduce foreign intelligence techniques against the American people, Congress must set the record straight. In order to bolster the traditional "line at the border" between foreign and domestic intelligence operations even further, Congress should also provide the PCLOB with explicit oversight authority over the NCTC and, for added measure, should require the NCTC to appoint a privacy or civil rights officer as envisioned in H.R. 1310.

Third, Congress should resolve any ambiguity created by the Intelligence Reform Act regarding the Attorney General's role in the FBI's domestic intelligence activities. Specifically, Congress should amend the Act to clarify that the Attorney General's traditional oversight role has not been usurped by the new DNI. The Center for National Security notes that, "[i]t is unclear whether the Attorney General's traditional authority over the FBI's intelligence activities has also been limited by provisions in the Intelligence Reform Act that grant the Director of National Intelligence (DNI) authority – not previously granted to the DCI – to task agencies of the intelligence community, including components of the FBI. Certainly there has been no

[90] THE 9-11 COMMISSION REPORT, *supra* note 41, at 423.
[91] *Id.*

public debate about the desirability of such changes."[92] In support of this proposition, the Center compares Section 103(c)(2) of the Act which provides that the DNI shall "(ii) determine requirements and priorities for, *and manage and direct the tasking of, collection, analysis, production and dissemination of national intelligence* by elements of the intelligence community," with Section 103(c)(2) of the original National Security Act, which simply requires the DCI to "establish the requirements and priorities to govern the collection of national intelligence by elements of the intelligence community."[93]

For the same reasons as those previously described, Congress never intended to dilute the Attorney General's oversight authority regarding the FBI's activities. On the contrary, Congress' purpose in creating the DNI was to promote greater coordination of the nation's intelligence effort, not to undermine an effective system of checks and balances.[94] To the extent some might read the Act to mean that the DNI can exempt the FBI from traditional restrictions on domestic intelligence operations, Congress must dispel this notion. Exempting the FBI from Attorney General oversight under any circumstances would rightly feed the public's concern that the NCTC might put privacy rights at risk.

Conclusion

Neither the NCTC nor the Intelligence Community can afford to lose the trust of the American people – a serious risk given recent revelations about how the Bush Administration is executing the war on terror both at home and abroad. By guaranteeing the strength and independence of the DHS Privacy Office through needed reforms; by bolstering the PCLOB and explicitly assigning it oversight of the NCTC; by clearly delineating the privacy obligations of

[92] Center for National Security Studies, *supra* note 49.
[93] *Id*. (citing Intelligence Reform Act, 50 U.S.C. 402 *et seq*., § 103(c)(2) and National Security Act, 50 U.S.C. 401 *et seq*., § 103(c)(2)) (emphasis added).
[94] THE 9-11 COMMISSION REPORT, *supra* note 41, at 411.

the NCTC and its constituent agencies; and by reaffirming the Attorney General's authority over the FBI, Congress can ensure that America's faith in our efforts to defeat the terrorists will not waver. If we fail to respect the rights of our citizens, however, we risk winning the war on terror without their cooperation, confidence, or commitment – a hollow victory indeed.