Statement of Christopher R. Calabrese, Legislative Counsel

American Civil Liberties Union

Washington Legislative Office

On

State Of Federal Privacy and Data Security Law: Lagging Behind the Times?

Before the Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

July 31, 2012

Good morning Chairman Akaka, Ranking Member Johnson, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the importance of updating the Privacy Act and assuring accountability and oversight regarding how the federal government handles personal information.

I. Introduction

The Privacy Act of 1974 was a landmark statute that has provided significant privacy protections but now needs to be updated. The Act formed the foundation for information privacy law, not just in the United States but around the world. The principles it delineates – the Fair Information Practices – have been written into law in almost every industrialized nation. They are the baseline best practices for anyone who gathers personal information – including governments and corporations. The practices require transparent descriptions of the information collected and grant the data subject control over how information is used and shared.[1]

The Privacy Act translates the fair information practices into a series of federal agency responsibilities and rights for individual citizens. Specifically, the Act controls when records can be collected and when and how they can be disclosed; allows individuals to access and correct their own records; and requires agencies to notify people about these systems and keep secure, accurate records.

However, even with this strong foundation, significant challenges have arisen in protecting personal privacy in the United States, including the data held by federal agencies. Some of these challenges arise from the age of the Privacy Act. Congress has not kept the Act up to date with existing technologies and new methods of disclosures such as data breach notification. Other challenges come from agency efforts to circumvent the Act through common practices such as boilerplate notices and the widespread use of commercial information. Still others arise from new court decisions that limit the recovery of damages under the Act.

Many of these problems are highlighted by the National Counterterrorism Center's (NCTC) recent decision claiming wide ranging authority to collect and use the personal, non-terrorist, information of innocent Americans for counterterrorism and law enforcement investigations.

This testimony is divided into four parts:

1. Updates to the Privacy Act;
2. Federal data breach notification;
3. Privacy Act remedies and oversight; and

[1] The full description of these principles can be found here: OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980).

4. Increased use of non-terrorism related information by the National Counterterrorism Center

I will discuss each of these problems in turn and provide recommendations to eliminate or mitigate them.

II. Updates to the Privacy Act

In 2008, this committee held a hearing, Protecting Personal Information: Is the Federal Government Doing Enough?, which explored many of the longstanding problems with the Privacy Act. Specifically, the testimony of Ari Schwartz from the Center for Democracy and Technology described several problems with the Privacy Act and privacy protections across federal agencies.[2] These issues have also been the focus of numerous studies by the US Government Accountability Office (GAO).[3] Longstanding issues include:

- the limited definition of "system of records",
- overuse of the "routine use" exception,
- failure to extend the protections of the Privacy Act to the government's use of commercial databases,
- shortcomings in agency compliance with the requirements of the E-Government Act of 2002 in regard to promulgating Privacy Impact Assessments, and
- the lack of privacy leadership at the Office of Management and Budget (OMB) and in some agencies.

Each of these problems persists four years later. I expect other members of the distinguished panel to describe them in detail. Rather than duplicate those efforts I will briefly highlight some key areas of focus.

System of records. The Privacy Act regulates "systems of records" and anything that falls outside of that scope is not regulated by the Act.[4] Unfortunately, this definition is unduly restrictive because it is tied to the process of retrieving information about a specific individual or information tied to that individual. Current technologies allow for a variety of search techniques using a range of criteria that are not tied to an individual. In discussing this problem, the GAO has noted "a data-mining system that performs analysis by looking for patterns in personal

---

[2] *Protecting Personal Information: Is the Federal Government Doing Enough": Hearing before the S Committee on Homeland Security and Governmental Affairs*, 110th Cong. (2008) (Statement of Ari Schwartz, Vice President, Center for Democracy & Technology) available at: http://www.hsgac.senate.gov/hearings/protecting-personal-information-is-the-federal-government-doing-enough

[3] GAO, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* GAO-08-795T (Washington D.C.: Jun 18, 2008); GAO, *Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603, (Washington D.C.: May 30, 2008).

[4] System of records is defined as "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 U.S.C. 552a(a)(5).

information located in other systems of records or that performs subject-based queries across multiple data sources may not constitute a system of records under the act."[5]

Routine Use. The routine use exception to the Privacy Act's disclosure provisions allows agencies to disclose information from systems of records without first obtaining consent from the individuals whose privacy is impacted. Although Congress intended this exception to permit records sharing only when "proper and necessary,"[6] the exception has become a catchall used to justify a wide array of disclosures. Seemingly, agencies are bound only by what they publish in the Federal Register as a routine use. The statutory requirement that disclosures be "compatible with the purpose for which [the information] was collected"[7] has been largely ignored. Thus, in practice, the routine use exception serves to circumvent the purpose of the Privacy Act by allowing disclosures at an agency's whim.

Commercial Databases. The Privacy Act does not extend to the federal government's use of commercial databases, despite the fact that such use has become widespread and prolific.[8] These databases frequently contain incorrect information and offer few of the protections, such as access, notice, correction and purpose limitations, which are fundamental to the Privacy Act and fair information practices. In spite of these shortcomings, commercial databases are often accessed for a wide variety of purposes by law enforcement and other agencies, including as part of background check investigations.[9]

Privacy Act Notifications. While agencies have made improvements in providing Privacy Impact Assessments (PIA) and System of Record Act Notices (SORN) for their databases, these notifications are frequently hard to find and often consist of boilerplate language which does a poor job of describing the actual uses of the database and how they handle personal information.[10] This information is sometimes scattered across agency websites and is difficult to find and understand.

Agency Leadership on Privacy. Since 2005 when agency privacy officers' authority was expanded and formalized, agencies have made strides in adding expertise and leadership on privacy.[11] However, in too many agencies, the title of Chief Privacy Officer is held by a senior agency level official such as the Chief Information Officer or General Counsel, but the actual

---

[5] GAO-08-795T, page 15.

[6] LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 967 (Joint Comm. on Gov't Operations ed., 1976) *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

[7] 5 U.S.C. § 552(a)(a)(7).

[8] See for example GAO, *Privacy: Government Use of Data From Information Resellers Could Include Better Protections*, GAO-08-543T (Washington D.C.: March 11, 2008).

[9] For more please see the ACLU statement on regulation of data aggregators: http://www.aclu.org/technology-and-liberty/letter-support-s-1490-personal-data-privacy-and-security-act

[10] United States. White House. Office of Management and Budget. *Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. Washington: GPO, 2012.

[11] 42 USC 2000ee-1.

privacy related responsibilities are handled by a much lower ranking official. Similarly, in spite of OMB's wide ranging responsibilities over privacy, the agency maintains no central privacy officer. These deficiencies result in fragmentation of the responsibility for maintaining privacy protections and uneven compliance with privacy related statutes and regulations.[12]

Recommendation: Each of these important and longstanding problems would be addressed in significant part by S.1732, Privacy Act Modernization for the Information Age Act of 2011. The ACLU believes passage of the portions of this legislation addressing these issues would be an important step forward in updating the Act and improving privacy in federal agencies.

III. Federal data breach notification

Breaches of data are an ongoing and serious problem. According to records compiled by Privacy Rights Clearinghouse, since 2008 at least 78 breaches of information held by federal agencies have occurred, compromising at least 77 million records.[13] However, existing OMB guidance on data breaches at federal agencies is inadequate and leaves too much discretion to individual agencies in determining whether to disclose breaches.

Relying on the Privacy Act as well as federal data privacy laws, the OMB memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (*M-07-16) directs federal agencies to implement a data breach notification policy by September 22, 2007 and outlines the framework for doing so.[14] The memorandum is split into four parts, each titled "attachment," which cover the treatment of personally identifiable information (PII), security requirements, outside notification in cases of a breach, and consequence of failures in agency compliance. This guidance only applies to federal executive agencies.

There is significant room for improvement in this guidance. On the positive side, it is mandatory for all agencies, requires basic security protections such as encryption, and advocates that agencies adopt privacy best practices such as data minimization and access limitations. It also prescribes a review of existing databases to assure that their contents are still relevant and necessary and requires the elimination of unnecessary uses of social security numbers. These requirements are particularly important for controlling sensitive information and reducing identity theft.

Where major problems arise with the guidance is in its recommendations for when affected individuals should be notified in the event of a data breach. In contrast to many state

---

[12] GAO, *Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603 (Washington D.C.: May 2008).

[13] *Chronology of Data Breaches*, Privacy Rights Clearing House, http://www.privacyrights.org/data-breach (unselect BSO, BSF, BSR, EDU and MED, unselect years 2005-2007, then hit "go").

[14] Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 *(*M-07-16).

data breach laws which mandate disclosure whenever data is lost, the OMB guidance describes an elaborate risk based trigger where the agency is required to evaluate a series of factors before determining whether to provide notification. In and of itself this type of discretion is very troubling. By their very nature data breaches are embarrassing events for agencies (or any entity) because they often reveal mistakes or poor security practices. Making notice discretionary will give the agency a strong incentive to come down on the side of not providing notice.

The factors and guidance OMB offers agencies in making this determination only exacerbate this problem. For example, part of the background OMB offers to the agency in deciding whether to disclose a breach is:

> "**Chilling Effects of Notices.** A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public. In addition, agencies should consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.[15]

It is hard to see how this guidance comports with the fundamental Privacy Act principle of transparency and accurate description of disclosures of records. In fact, it seems like an active invitation to defer notice.

The key criteria OMB offers for determining whether to provide notice are equally problematic. As an initial matter, OMB frames all breach notification requirements in terms of whether the breach is likely to cause harm and the level of risk associated with that harm. While harm is an important criteria, it ignores the other important role that public breach notification plays, namely as an accountability tool that spurs improved security and privacy controls. Small breaches are often indicative of a larger problem in computer security practices, training or other controls. Allowing agencies to paper over those problems is likely to lead to greater problems down the road.

Further, OMB's evaluation of what might cause harm is flawed. It encourages agencies to consider factors like:

> the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.[16]

[15] *Id* at 12-13.
[16] *Id* at 15.

These decisions are best made by the individual affected, not the agency. In reality, it is impossible to see how the agency could foresee secondary uses of data. Sometimes even data that most people view as benign, such as name and address, can be very sensitive if associated with a survivor of sexual assault or stalking who has worked very hard to conceal it.

The guidance also authorizes the agency to consider whether the risk can be mitigated by the agency. Naturally the agency should take all mitigation steps but that effort should be completely separate from a decision about whether to notify victims of a breach. Again, all of this guidance is completely contrary to the fundamental purpose of the Privacy Act: to empower citizens with knowledge about and control over how the government handles their personal information.

Recommendation: OMB should change its data breach guidance to severely limit the discretion of federal agencies to avoid providing notice to affected parties in the case of a breach. Notice should be triggered whenever personally identifiable data is released in a readable form (not protected by encryption or other security measures).

IV. Privacy Act Remedies and Oversight

Since 2008, there have been two significant developments which have served to further erode transparency and accountability under the Privacy Act – the recent Supreme Court case *FAA v. Cooper* and the failure by the President and Congress to fill the Privacy and Civil Liberties Oversight Board (PCLOB).

A. FAA v. Cooper

In *FAA v. Cooper*, the Supreme Court held that the victims of Privacy Act violations cannot recover damages for mental or emotional distress, no matter how severe, unless they suffer financial harm as a result of the violation.[17] In *Cooper*, the plaintiff's HIV status was shared by the Social Security Administration with the Federal Aviation Administration (FAA) and Department of Transportation.

In *Cooper*, despite the fact that the agencies violated the Privacy Act, it was unclear whether the plaintiff could recover the damages authorized by 5 U.S.C. 552(a)(g)(4)(A). This section provides that any agency who willfully fails to comply with the Privacy Act is liable for "actual damages sustained by the individual as a result of the… failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000." At issue was the definition of "actual damages." In previous decisions, circuits had split over whether "actual damages" meant "general damages," which allow recovery for emotional harm, or "special damages," which required pecuniary harms.[18] This definition was important because the plaintiff did not allege an

[17] *F.A.A. v. Cooper*, 132 S. Ct. 1441 (2012).

[18] *See Fitzpatrick v. IRS*, 665 F.2d 327, 329-31 (11th Cir.1982) (holding that "actual damages" are limited to proven pecuniary losses); *Johnson v. IRS*, 700 F.2d971, 972 (5th Cir. 1983) (holding that "actual damages" may be

economic loss as a result of the Privacy Act violation. He only claimed to have suffered "humiliation, embarrassment, mental anguish, fear of social ostracism and other severe emotional distress."[19] The Court concluded that Congress intended through use of the term "actual damages" to mean special damages and limited the availability of recovery under the Privacy Act to those suffering from economic harm. The plaintiff was denied damages for his emotional harm.

This decision has a negative impact on the general privacy protections provided by the Act, as well as on an individual's ability to recover for harms. The Privacy Act was created in order to provide "a series of basic safeguards… to help remedy the misuse of personal information by the Federal Government and reassert the fundamental rights of personal privacy of all Americans."[20] Congress viewed the civil damages remedy as key to enforcing the Act and as commentators have noted the deterrent effect presented by the threat of litigation is a significant one.[21] By foreclosing relief for these types of harms, the court weakens protections for precisely the type of harmful disclosure of embarrassing or detrimental information, such as HIV status, that should be a core focus of the Act.

The decision also strips from victims of real harms the ability to recover their damages. The court's holding is clear. No matter how much emotional pain, humiliation or real mental distress a victim endures, if it is not a pecuniary harm, recovery is barred. In practice the result of this interpretation is that release of much of the information covered by the Privacy Act will fall outside the statutory remedy. For example, recently it was alleged that the 2010 campaign of Washington, D.C. Mayor Vincent Grey improperly used lists of residents of public housing as part of its get out the vote efforts.[22] These lists would be covered by the Privacy Act and contain names, addresses and phone numbers including cell phones. If public housing residents were harmed by this disclosure, for example by receiving harassing phone calls, under *Cooper* they would have no remedy absent a showing of financial harm.

Recommendation: The language of the Privacy Act should be modified in 5 U.S.C. 552a(g)(4)(A) to make clear that actual damages extend beyond pecuniary harms and include mental and emotional distress.

B. Privacy and Civil Liberties Oversight Board

---

established by evidence of either financial or non-financial injuries); *Hudson v. Reno*, 130 F.3d 1193, 1206-07 (6th Cir. 1997) (holding that "actual damages" can be established only by evidence pecuniary losses).

[19] *Cooper* at 1447.

[20] *House Comm. on Gov't Operations and Senate Comm. on Gov't Operations*, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 -- S. 3418 (Pub. L. No. 93-579) Source Book on Privacy, 304 (1976) *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

[21] Frederick Z. Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611, 622 (1984).

[22] Nikita Stewart and Mike DeBonis, *Mayor Gray's 2010 campaign had database of public-housing residents*, Washington Post, July 22, 2012.

At the recommendation of the 9/11 Commission, in 2004, Congress created the Privacy and Civil Liberties Oversight Board (PCLOB) and later reconstituted it as an independent body in 2007.[23] The PCLOB is tasked with overseeing "the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they appropriately protect privacy and civil liberties".[24] As such, it has significant oversight authority regarding the type of collection and sharing of personal information regulated by the Privacy Act and could serve as an important check on abuses of the Act.

Unfortunately, President Bush refused to nominate one of the candidates put forth by leaders in Congress who traditionally select the commissioners from the opposite party from the president. In retaliation, the Senate refused to confirm any of Bush's GOP nominees. Because the terms of the original board members expired in January 2008, the revised board was never brought into existence during President Bush's term.[25]

Compliance has been no better under President Obama. Despite letters from lawmakers and advocacy groups, he failed to nominate a full slate of candidates for the Board for almost three years. It wasn't until December 2011 that nominations were sent to the Senate for its consideration.[26] Candidates for the PCLOB have been awaiting action by the full Senate since May.

Given that the board has never existed in its current form it is hard to concretely evaluate the impact it would have on Privacy Act enforcement, however it was a key recommendation of the 9/11 Commission. As the former Chairman Tom Kean and Vice Chairman Lee Hamilton testified before this committee:

> If we were issuing grades, the implementation of this recommendation would receive a failing mark. We urge the Administration and Congress to address this failure in a speedy fashion. An array of security-related policies and programs present significant privacy and liberty concerns. A robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind.

---

[23] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 395. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-408 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801 (2007).

[24] The 9/11 Commission Act of 2007 §801 (d)(2)(B).

[25] Michael Isikoff and Mark Hosenball, "Who's Watching the Spies?" *Newsweek*, July 9, 2008; online at http://www.newsweek.com/id/145140.

[26] The White House, Office of the Press Secretary, *President Obama Announces More Key Administration Posts*, December 15, 2011.

> Board review can also give national security officials an extra degree of assurance that their efforts will not be perceived later as violating civil liberties.[27]

While it is unknown how much oversight the PCLOB will eventually exert, it is incontrovertible that it will be impossible for the Board to provide any oversight until members are nominated and confirmed.

Recommendation: Nominate and confirm a full slate of board members for the PCLOB and fully staff this vital independent board.

V. Increased use of non-terrorism related information by the National Counterterrorism Center

The steady erosion of privacy protections for personal information held by the federal government has led to an environment where information on Americans can be shared widely for a host of purposes unrelated to the original reason it was collected. Perhaps the most troubling recent example of this trend is the sweeping changes the National Counterterrorism Center (NCTC) made to its guidelines governing how it collects and uses information about US persons not suspected of wrongdoing for intelligence analysis.[28] The new rules effectively remove traditional protections for US person information and allow the vast power of the US Intelligence Community to be turned on innocent Americans. They clearly demonstrate the need to update the Privacy Act and ensure that Americans have real protections for how the information collected by an array of federal government agencies is shared and used.

A. Changes to the NCTC Guidelines

Under the new guidelines approved by the Attorney General, NCTC may engage in a variety of troubling new practices including collecting entire databases from federal agencies which mainly consist of information about Americans with no connection to terrorism, and analyzing those databases and disseminating the results for reasons which are also unconnected to terrorism.

The new guidelines accomplish this in a variety of ways. In what is perhaps the most significant change, the Obama administration has extended the authority of the NCTC to intentionally collect, retain and assess data on U.S. citizens and residents, even where those people have no suspected ties to terrorism. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or related to an actual investigation. Therefore, when NCTC collected information from federal

---

[27] *Ten Years After 9/11: A Report From the 9/11 Commission Chairmen, before the Senate Committee on Homeland Security and Governmental Affairs*, 112th Congress, (2011) (Testimony Governor Tom Kean and Congressman Lee Hamilton).

[28] National Counterterrorism Center, GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, Released March 22, 2012.

government databases, it had to search for and identify any innocent US person information inadvertently collected, and discard it within 180 days. This crucial purpose limitation meant that NCTC was dissuaded from collecting or maintaining information on innocent Americans in its large databases, and prohibited from using or disseminating it. The 2012 guidelines eliminate this check, allowing NCTC to collect and "continually assess" information on innocent Americans for up to five years.[29]

The new guidelines also effectively broaden an authority previously claimed by NCTC, namely the ability to ingest entire databases maintained by other government agencies. According to the new guidelines, as long as the Director of the NCTC determines that a dataset contains "significant terrorism information," which is not defined, the NCTC may "acquire and replicate portions or the entirety of a dataset". While NCTC previously claimed such authority, the retention limits on collection for US persons meant that only datasets consisting almost entirely of terrorism information and/or non-US person information could reasonably be collected using this methodology. The NCTC was dissuaded from swallowing up entire databases consisting of large amounts of innocent US person information by the resource burden of locating and purging it within 180 days. By allowing collection and retention of non-terrorism related US person information for 5 years, the NCTC Guidelines have authorized the NCTC to ingest many new federal databases that consist primarily of non-terrorism related US person information.[30]

Once NCTC acquires this information, the new guidelines give it broad new powers to search through it. As long as queries are designed to solely identify information that is reasonably believed to constitute terrorism information, it may conduct queries that involve non-terrorism data points and pattern based searches and analysis (data mining).[31] It is particularly noteworthy that NCTC relies on a technique, data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be caught up in terrorism investigations if this technique is utilized. As far back as 2008 the National Academy of Sciences found that data mining for terrorism was scientifically "not feasible" as a methodology, and likely to have significant negative impacts on privacy and civil liberties.[32]

Equally disturbing is that once information is gathered and assessed with these tools it can be shared very broadly, in some cases with literally anyone. Such sharing does not have to

[29] 2012 Guidelines at 9.
[30] *Id*.
[31] *Id* at 10.
[32] *See* National Academy of Sciences report, "Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment" http://books.nap.edu/catalog.php?record_id=12452#toc

be connected to a terrorism investigation. This chart lists some of the types of information NCTC may share, as well as all the entities that can receive this information:[33]

Types of information that can be shared	**Individuals and groups that can receive information**
Foreign aspects of international narcotics activities	Federal, state, local, tribal, or foreign or international agency that is reasonably believed to need such information
Reasonably appears to be evidence of a crime	Federal, state, local, tribal, or foreign agency which has jurisdiction and that is reasonably believed to need such information
Reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations or (ii) protect against or prevent a crime or a threat to the national security	Federal, state, local, tribal, or foreign entity, or to an individual or entity not part of a government
For the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts	Federal, state, local, tribal, or foreign or international entity
For the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure	Federal, state, local, tribal, or foreign or international entity
Otherwise required by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements	2012 Guidelines are silent on who the sharing would be to, but presumably that would be covered by the statutes, treaties, orders, directives, policies, MOUs or agreements
For the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it	Appropriate elements of the Intelligence Community
Bulk dissemination in support of a legally authorized counterterrorism mission	Other elements of the Intelligence Community

In short, information can be shared for an almost unlimited number of purposes and to a completely unlimited number of individuals. Particularly striking is the authority to share information with anyone ("federal, state, local, tribal, or foreign entity, or to an individual or

[33] *Id* at 13-14.

entity not part of a government") in order to protect the safety or security of person, property or organizations; or protect against or prevent a crime or a threat to the national security. Such authority seems to provide few limits and almost no guidance to NCTC and other intelligence agencies.

All of this is happening with very little oversight. Controls over the NCTC are mostly internal to the DNI's office and important oversight bodies such as Congress and the President's Intelligence Oversight Board aren't notified of even "significant" failures to comply with the Guidelines.[34] One entity might be able to perform some useful oversight because it does have fairly straightforward authority to "access all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other materials that it deems relevant to its oversight of NCTC activities." Unfortunately that entity is the PCLOB, which, as described above, has not been seated.

B. Privacy Act Impact

When these practices are viewed through the lens of the supposed protections of the Privacy Act, it is clear how badly the Act is in need of an update. One of the major protections of the Privacy Act is that it bars the sharing of records between agencies except pursuant to specifically delineated exceptions described in subsection (b). None of these exceptions are broad enough to cover this type of wholesale disclosure to the NCTC, nor is there a general national security exception to the Privacy Act. Presumably then, entire databases are being disclosed pursuant to the long abused "routine use" exception described in section II. However, it is difficult to imagine that any American believes that any transaction with the federal government can open them up for screening as a terrorist as long as an agency declares use of that information for that purpose to be "routine".

Courts have also held that agencies shouldn't share information with other agencies unless it has compatibility with the purpose for which the information was collected The modern definition of "compatibility" was established in *Britt v. Naval Investigative Services,* in which the 3rd Circuit held there must be "some meaningful degree of convergence between the agencies' purpose in collecting the information and its disclosure."[35] The court also noted that the purpose for collection and disclosure should be determined on a case-specific basis. Similarly, in *Swenson v. U.S. Postal Service*, the 9th Circuit echoed *Britt's* holding, and found that there must be a "meaningful degree of convergence" between the purpose for which the information was collected and the reason it was disseminated.[36]

[34] *Id* at 17.
[35] 886 F.2d 544 (3rd Cir. 1989)
[36] 890 F.2d 1075 (1989)

The NCTC also asserts a series of other exceptions to the Privacy Act. These types of exemptions are authorized under subparts (j) and (k) of the Act and have become commonplace. But a quick review of the exemptions NCTC asserts demonstrates how much control they take away from the subject of the information. NCTC exempts itself from the following requirements for all its databases:

- Subsection (c)(3) (accounting for disclosures),
- Subsections (d)(1)-(4) (record subject's right to access and amend records),
- Subsection (e)(1) (maintain only relevant and necessary records),
- Subsection (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents),
- Subsection (e)(4)(I) (identifying sources of records in the system of records), and
- subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees).[37]

In short, NCTC will not guarantee it is using accurate information, account for how it discloses that information, assure that it is relevant or ever let individuals know they have been the subject of an investigation. For obvious reasons the accuracy of the information is of particular concern. Evidence from other database where the collecting agency does not attest to the accuracy of the information indicates that this tends to result in substantial errors.[38]

The federal government collects an enormous amount of personal information. It is necessary in order for citizens to receive benefits and services, to exercise fundamental rights like voting or petitioning the government, for licensing everything from guns to businesses, for employment, education and for many types of health care. In short this information collection is nearly ubiquitous to American life. However under the new NCTC guidelines and the outdated protections of the Privacy Act, providing this information to any federal agency is akin to entering a lineup as a potential terrorist. Nor does the government's sharing this information have to be connected to terrorism at all. Information can be used for national security and safety, drug investigations, if it is evidence of a crime, or simply to evaluate sources or contacts. This boundless sharing is broad enough to encompass disclosures to an employer or landlord about someone who NCTC may think is potentially a criminal, or at the request of local law enforcement for vetting you as a potential informant.

Ultimately, this boundless disclosure, limitless sharing and expansive exemptions seem to create a system of records that is outside the Privacy Act. The only protection offered by the Privacy Act in regard to NCTC is strictly bureaucratic – the agency must declare that a system of records exists and, either explicitly state that many of the provisions of the Privacy Act do not

[37] 32 CFR 1701.21

[38] See for example errors in the National Crime Information Center (NCIC) which is collected by the FBI: http://bjs.ojp.usdoj.gov/content/pub/pdf/umchri01.pdf and http://epic.org/privacy/hiibel/epic_amicus.pdf

apply or implicitly exploit loopholes to avoid its requirements. Contrast this with the Congressional finding in support of the Privacy Act:

> The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information; … In order to protect the privacy of individuals identified in information system maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

It is difficult to see how the NCTC's guidelines for handling Americans' personal information meet any of these goals. Unfortunately, this type of broad information sharing is not an isolated occurrence. Instead, broadening definitions of routine use, constant employment of exemptions, use of commercial databases and boilerplate notifications result in a systematic weakening of the Privacy Act and widespread harm to Americans privacy.

Recommendation: Congress should prohibit the intelligence community's intentional collection of non-terrorism related US person information. If such information is inadvertently collected it should be immediately identified and removed.

VI. Conclusion

The Privacy Act and other associated federal data use practices require an overhaul. Their outdated protections are widely circumvented by agencies and the result is the creation of new databases, such as those compiled by the NCTC that violate the spirit of the Privacy Act and harm Americans' privacy.