The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2769 | FEBRUARY 21, 2013

New National Counterterrorism Center Guidelines Require Strong Oversight

John G. Malcolm, Jessica Zuckerman, and Andrew Kloster

Abstract
The new guidelines on data sharing and retention of "terrorism information" in federal databases expand the ability of the National Counterterrorism Center (NCTC) to access, retain, and analyze data to help to thwart terrorist attacks. Given recent terrorist actions, such as the 2009 Fort Hood attack and the attempted Christmas Day bombing, the new guidelines are needed. However, to protect the rights of American citizens, Congress should ensure that existing internal and external controls are being followed.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2769**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

In March 2012, the Director of National Intelligence (DNI), the U.S. Attorney General, and the director of the National Counterterrorism Center (NCTC) developed updated guidelines on data sharing and retention of "terrorism information" in federal databases.[1] These new guidelines, which have not yet been implemented, were spurred in part by the counterterrorism failures surrounding the 2009 Fort Hood attack and that year's attempted Christmas Day bombing. They expand the NCTC's ability to access, retain, and analyze data in government databases in searching for information that could help to thwart terrorist attacks.

Since 9/11, at least 54 publicly known Islamist-inspired terrorist plots against the United States have been thwarted. While a few of these plots were foiled by luck or the swift action of everyday citizens, the vast majority were thwarted by robust U.S. intelligence efforts.[2] It is essential to ensure that America's counterterrorism and intelligence authorities have the tools they need to stop terrorists long before the public is put in danger.

Of course, any expansion of government data retention and usage needs to be accompanied by sufficient oversight to protect the privacy

Key Points

- The National Counterterrorism Center (NCTC) serves a critical function in the intelligence community, serving as a clearinghouse for all national counterterrorism intelligence.
- New NCTC guidelines, which have been approved but not yet implemented, will expand the NCTC's ability to access, retain, and analyze data contained in government databases in search of information that could help to thwart future terrorist attacks.
- It is essential to ensure that U.S. counterterrorism and intelligence authorities continue to have the tools they need to help stop terrorists long before the public is put in danger.
- To ensure that the NCTC is respecting the legitimate privacy rights and civil liberties of people living in the United States, Congress should provide effective oversight to verify that the NCTC is using its expanded authority appropriately.
- National security is of the utmost importance, but so is individual liberty.

and other rights of American citizens. Thus, as the new NCTC guidelines move toward implementation and even once they are implemented, Congress should ensure that the NCTC and other agencies in the intelligence community have the tools they need to thwart terrorist attacks before they occur, while still conducting regular and rigorous oversight hearings to ensure that the legitimate privacy and other rights of people living in this country are respected.[3]

Breaking Down Intelligence Stovepipes

In its final report, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) highlighted an unwillingness to share information within the U.S. intelligence community. A remnant of the Cold War "need to know" culture, the risks of inadvertent disclosure were viewed as outweighing the benefits of broader information sharing.[4] As a part of the solution, the commission called for decentralizing information networks, allowing databases to be searched across agency lines. The commission also called for the creation of the NCTC to serve as a center for joint intelligence and operational planning.

In August 2004, just weeks after the release of the 9/11 Commission's final report, President George W. Bush issued Executive Order 13354, creating the NCTC. A few months later, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) codified the NCTC's creation.

The IRTPA was also enacted, in part, to authorize agencies to release "terrorism information" produced by "intelligence, law enforcement, military, homeland security, or other activities."[5] While not altering the preexisting jurisdiction of agency heads over their own information, the IRTPA sought to facilitate an "Information Sharing Environment" by reducing disincentives to share information between agencies and providing affirmative incentives to do so. To assist in implementing the IRTPA, President Bush issued Executive Order 13388 on October 25, 2005, further directing the heads of federal agencies to enhance information sharing on terrorist threats.

Even now, key challenges still exist in breaking down intelligence stovepipes and connecting the dots. Indeed, two of the most poignant examples in recent memory relate to the successful terrorist attack at Fort Hood and the nearly successful Christmas Day bombings in 2009. In both cases, the intelligence community and Congress identified "the government's limited ability to query multiple federal datasets and to correlate information from many sources that might relate to a potential attack."[6] Indeed, a Senate report analyzing the situation surrounding the thwarted Christmas Day attack attributed some of the blame to the intelligence community's failure to "connect the reporting" on the Christmas Day bomber, Umar Farouk Abdulmutallab, and recommended that the DNI develop and employ "advanced information technology," such as "pattern-based queries," to draw connections among intelligence reports and to notify

1. U.S. Department of Justice, "Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Databases Containing Non-Terrorism Information," 2012, http://www.nctc.gov/docs/NCTC%20Guidelines.pdf (accessed January 29, 2013). See also Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485 (2012). The NCTC is working toward implementing these new guidelines, but will need to do much legwork before implementing them. For example, internal compliance procedures must be developed or refined to ensure compliance with the new safeguards and compliance requirements of the 2012 Guidelines, and new information-sharing agreements with provider agencies must be secured to the extent necessary to comply with the new rules.
2. James Jay Carafano, Steven P. Bucci, and Jessica Zuckerman, "Fifty Terror Plots Foiled Since 9/11: The Homegrown Threat and the Long War on Terrorism," Heritage Foundation *Backgrounder* No, 2682, April 25, 2012, http://www.heritage.org/research/reports/2012/04/fifty-terror-plots-foiled-since-9-11-the-homegrown-threat-and-the-long-war-on-terrorism.
3. Consistent with this purpose, the DNI has issued a report outlining the privacy protections in the 2012 Guidelines: Office of the Director of National Intelligence, Civil Liberties and Privacy Office, "Description of Civil Liberties and Privacy Protections Incorporated in the Updated NCTC Guidelines," January 2013, http://nctc.gov/docs/CLPO_Information_Paper_on_NCTC_AG_Guidelines_-_1-22-13.pdf (accessed January 29, 2013).
4. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), http://govinfo.library.unt.edu/911/report/index.htm (accessed February 13, 2013).
5. In addition to leaving preexisting jurisdiction intact, the IRTPA did not envision any intelligence-gathering function for the NCTC. See John O. Brennan, "Responses from John O. Brennan to Post-Hearing Questions," letter to Representative John Conyers Jr., Ranking Democratic Member, Committee on the Judiciary, U.S. House of Representatives, December 4, 2003, http://www.fas.org/irp/agency/ttic/qfr120403.pdf (accessed January 29, 2013).
6. Office of the Director of National Intelligence and U.S. Department of Justice, "Revised Guidelines Issued to Allow the NCTC to Access and Analyze Certain Federal Data More Effectively to Combat Terrorist Threats," March 22, 2012, http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/528-odni-and-doj-update-guidelines-for-nctc-access,-retention,-use,-and-dissemination-of-information-in-datasets-containing-non-terrorism-information (accessed January 29, 2013).

congressional intelligence committees of its progress on that front.[7] These findings led to the promulgation of the 2012 Guidelines, which were made public in March.

New NCTC Guidelines

The new 2012 NCTC Guidelines make several changes to the previous guidelines governing the NCTC's retention, use, and dissemination of "terrorism information" within federal databases, specifically those databases identified as containing non-terrorism information and information pertaining to domestic terrorism.[8]

Perhaps the most significant change is that the NCTC is now authorized to request and store databases from other agencies containing non-terrorism information in order to conduct "pattern-based queries and analyses." The 2008 Guidelines explicitly prohibited pattern-based queries. Terrorism information as defined by statute refers to information collected by the government relating to specific terrorist groups or activities.[9] Pattern-based queries (often called "data mining") involve analyzing non-terrorism information to establish patterns that may assist in identifying potential terrorists and halting plots early on.[10] A pattern-based query would thus involve a thorough search of available databases looking for particular combinations of factors, such as individuals who travel to particular countries where terrorist activity has been known to occur and who set up accounts in particular banks that terrorists have been known to use. By themselves, these factors may be perfectly innocent, but in combination they might suggest that additional investigation is warranted. Such queries of large datasets are distinguishable from "link analysis," which involves starting with a known or suspected terrorist connection involving a particular individual and conducting additional inquiries about that person to confirm or deny that connection.

PERHAPS THE MOST SIGNIFICANT CHANGE IS THAT THE NCTC IS NOW AUTHORIZED TO REQUEST AND STORE DATABASES FROM OTHER AGENCIES CONTAINING NON-TERRORISM INFORMATION IN ORDER TO CONDUCT "PATTERN-BASED QUERIES AND ANALYSES."

Under the 2012 guidelines, the NCTC can retain non-terrorism information for up to five years and query the data whenever it wishes to do so within that period.[11] However, if the information is deemed "terrorism information," the NCTC can retain such data beyond five years. The NCTC must still remove "all identified information concerning United States persons" not constituting terrorism information. Under the 2008 Guidelines, the NCTC was required to promptly review and remove non-terrorism information. The new guidelines also expand the NCTC's ability to share personal data with "any appropriate entity," which can range from local agencies to foreign governments in order to determine whether that data "constitutes terrorism information."

Comparative Privacy Models and Current Concerns

While these new guidelines make important changes to help the NCTC track and thwart terrorism, they have spurred some privacy concerns among the public and

7. U.S. Senate, Select Committee on Intelligence, "Unclassified Executive Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253," May 18, 2012, http://intelligence.senate.gov/100518/1225report.pdf (accessed January 29, 2013).
8. For a nuts-and-bolts overview by *The Wall Street Journal* that identifies the many ways in which the 2012 Guidelines differ from the 2008 Guidelines, see Julia Angwin, "A Comparison of the 2008 and 2012 NCTC Guidelines," *The Wall Street Journal*, December 12, 2012, http://blogs.wsj.com/digits/2012/12/12/a-comparison-of-the-2008-and-2012-nctc-guidelines (accessed January 29, 2013). See also U.S. Department of Justice, "Memorandum of Agreement Between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center of Terrorism Information Contained Within Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism," 2008, https://www.documentcloud.org/documents/490760-nctc-guidelines-2008.html (accessed January 29, 2013).
9. For the purposes of information sharing, "terrorism information" is defined broadly. See 6 U.S. Code § 485 (a)(5). This definition seems broad enough to ensure that if an agency can collect such information, it is likely authorized to disclose that information to the NCTC. For example, "terrorism information" is at least as extensive as the IRTPA amendments to the Foreign Surveillance Act that define "agent of a foreign power" as including "lone-wolf" terrorists: non-U.S. persons who "engage in international terrorism or activities in preparation therefore."
10. Any use of pattern-based queries is thus governed by the reporting requirements of the Federal Agency Data Mining Reporting Act of 2007, 52 U.S. Code § 2000ee-3, http://www.law.cornell.edu/uscode/text/42/2000ee-3 (accessed January 29, 2013). For an example of such a report in the national security context, see Office of the Director of National Intelligence, "2010 Data Mining Report," April 2011, http://www.fas.org/irp/dni/datamining11.pdf (accessed January 29, 2013).
11. Five years represents the maximum retention period allowed under the guidelines, but the retention period for any particular dataset might be limited by a statute governing the terms of retention of such data or by an agreement negotiated between the agency providing that data and the NCTC. Furthermore, the data, in turn, may have retention limitations imposed by international agreement.

some former government national security lawyers.[12] The United States has always had a strong and healthy strain of civil liberties and privacy protection, as it should and must. However, the United States protects that liberty in a system that differs from the European system of protections for historical and structural reasons. Although different societies treat privacy and civil liberties concerns in distinct ways, this difference is instructive.[13]

Europe's Privacy Paradigm. Among European countries, with their history of fascist and Communist regimes, the right to privacy is broad, and significant internal restrictions are imposed on how personal information is processed. A European Union (EU) directive strictly regulates the processing of personal data by commercial entities within the European Union.[14] In general, personal data can be processed only for specified, legitimate purposes and only insofar as it is relevant and not excessive in relation to that purpose—a concept known as proportionality. Additional restrictions apply to particularly sensitive personal data, such as religious beliefs, political opinions, sexual orientation, and membership in organizations. Perhaps most notably for purposes of comparison, the directive establishes strict rules and time limits on the retention of personal data.

By its terms, the current directive does not apply to law enforcement and counterterrorism activities and, like most European Commission directives, the privacy directive is implemented by each of the EU member states in differing ways.[15] Thus, in practice, privacy protection varies across the European Union. Nevertheless, the Data Protection Directive is emblematic of the strong thematic concern with which Europeans view privacy intrusions.

Indeed, in January 2012, the European Commission released a draft European General Data Protection Regulation, which, if adopted, would supersede the Data Protection Directive and extend the scope of existing data protection laws to all foreign companies that process data of EU residents and impose severe penalties on those who violate the directive. It may also, depending on the views of the European Parliament and the European Commission, formally extend the data protection regime to the law enforcement domain.

America's Approach to Privacy. While the United States has chosen, for the most part, not to follow the European model for data privacy, this does not mean that privacy rights in America are less securely protected. To the contrary, Americans are well aware that history is replete with examples of repressive governments that used secret police to keep close tabs on the activities of its citizens in order to repress them. Recent examples include East Germany's Stasi, Cuba's G2, and Chile's National Intelligence Directorate. Some might even include the FBI and the CIA in the 1950s and 1960s.[16]

WHILE THE UNITED STATES DOES NOT DEFINE PRIVACY IN THE SAME WAY AS THE EUROPEAN UNION, IT ACHIEVES MUCH THE SAME RESULT THROUGH A DUAL PROCESS OF PARTICULARIZED CONTROLS FOR DIFFERENT TYPES OF GOVERNMENT INVESTIGATIONS AND RIGOROUS OVERSIGHT.

While the United States does not define privacy in the same way as the European Union, it achieves much the same result through a dual process of particularized controls for different types of government investigations and rigorous oversight. For instance, in the context of domestic criminal law enforcement, the requirements of the Fourth Amendment, including the exclusionary rule, and other due process rights, which are subject to judicial review, provide extensive protection to criminal defendants.

12. Julia Angwin, "U.S. Terrorism Agency to Tap a Vast Database of Citizens," *The Wall Street Journal*, December 13, 2012, http://online.wsj.com/article/SB10001424127887324478304578171623040640006.html (accessed January 29, 2013).
13. Paul Rosenzweig and Michael Scardaville, "The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program," Heritage Foundation *Legal Memorandum* No. 6, February 6, 2003, http://www.heritage.org/research/reports/2003/02/the-need-to-protect-civil-liberties.
14. European Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal* L 281, November 23, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT (accessed January 29, 2013).
15. Case C-317/04, *Parliament v. Commission*, 2005 E.C.R. I-02467, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-318/04 (accessed February 13, 2013).
16. *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book III: Final Report Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, S. Rep. 94–755, 94th Cong., 2nd Sess., April 23, 1976, http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIa.htm (accessed January 29, 2013).

The expanded powers of the NCTC should be no exception. It is a core American principle of limited government that a free people should always approach any expansion of the government's ability to monitor its citizens with a healthy degree of skepticism. Even where the subject matter is national security, they should still insist upon appropriate controls on the front end as well as vigorous oversight by responsible individuals in both political branches of government to protect Americans' constitutional rights and right to privacy.

Privacy Concerns and Protections of the NCTC Guidelines. To that end, numerous civil liberties organizations have raised concerns about the 2012 Guidelines. These concerns largely critique the alleged ability of the government to obtain, retain, and analyze large amounts of non-terrorism and non-criminal information about average citizens, the vast majority of whom will be innocent, in an effort to find connections that might lead them to would-be terrorists.[17]

However, certain safeguards are already in place to monitor and prevent unnecessary and unwarranted invasions of privacy. While the United States does not protect privacy rights in the same way as in Europe, privacy rights are protected at least as well in the United States, if not more strongly than they are in Europe. Unlike the European privacy regime that relies solely on internal checks and administrative law, the United States protects privacy with an "all-of-the-above" regime that includes potential administrative and judicial remedies for violations, above and beyond those provided in the context of a criminal trial.

The IRTPA, Executive Order 13388, and the 2008 and 2012 Guidelines each explicitly defer to all "applicable law, including Federal law protecting information privacy and other legal rights of Americans."[18] Consequently, most general privacy concerns might already be mitigated by existing statute. Indeed, numerous existing statutes limit the scope of NCTC activities and provide serious oversight mechanisms for privacy violations, including providing monetary damages for illegal release of information.[19]

To a certain extent, privacy concerns related to the NCTC can be mitigated with ad hoc privacy limitations in subject-matter-specific titles. For example, if citizens consider privacy of health records to be very important, legislators can amend the Health Insurance Portability and Accountability Act (HIPAA), which would affect the ability of other federal agencies to release such information to the NCTC. The same can be done with other federal laws relating to specific privacy concerns. Similarly, data use by the NCTC can be limited by each specific data-sharing agreement signed by the NCTC and the agency releasing data.[20] For both of these reasons, enforcement can be directed against the agencies providing protected information rather than the agencies, such as the NCTC, receiving the information. Against the IRTPA's background presumption of information sharing, legislators, courts, and the public can debate the merits of privacy exceptions in specific cases.

In addition, both the statute and the 2012 Guidelines encourage the NCTC to self-police their new powers. For example, the 2012 Guidelines require the NCTC to request

17. Chris Calabrese, "Vast New Spying Program Was Started in Secret on a Bogus Pretext," American Civil Liberties Union, December 13, 2012, http://www.aclu.org/blog/national-security-technology-and-liberty/vast-new-spying-program-was-started-secret-bogus (accessed January 29, 2013), and Trevor Timm, "Government Attorneys Agree with EFF: New 'Counterterrorism' Database Rules Threaten Privacy of Every American," Electronic Frontier Foundation, December 19, 2012, https://www.eff.org/deeplinks/2012/12/government-attorneys-agree-eff-new-counterterrorism-database-rules-threaten (accessed January 29, 2013).
18. George W. Bush, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," Executive Order No. 13388, Sec. 7(a)(i), October 25, 2005, http://www.gpo.gov/fdsys/pkg/FR-2005-10-27/pdf/05-21571.pdf (accessed February 13, 2013).
19. Federal Agency Data Mining Reporting Act of 2007, 52 U.S. Code § 2000ee-3. The act explicitly requires federal agencies, including the NCTC, that engage in "data mining" as defined by the statute to submit an annual report to Congress, which is available to the public and includes "thorough descriptions" of the activities, relevant data, and legal authorization for such data mining. Privacy Act of 1974, 5 U.S. Code § 552a, http://www.justice.gov/opcl/privstat.htm (accessed January 29, 2013). The Privacy Act prohibits agencies from disclosing records and provides a private right of action to collect money damages for unauthorized information sharing. Health Insurance Portability and Accountability Act of 1996, Public Law 104–191, http://www.legalarchiver.org/hipaa.htm (accessed January 29, 2013). HIPPA regulates the release of protected health information by "covered entities," which include government health plans. Family Education Rights and Privacy Act of 1974, 20 U.S. Code § 1232g, http://www.law.cornell.edu/uscode/text/20/1232g (accessed January 29, 2013). The act protects the education records of students at education institutions, including military academies. In compliance with many of these provisions, the NCTC publishes privacy notices in the *Federal Register*.
20. Additionally, the NCTC, in consultation with the DNI, the DNI Civil Liberties Protection Office, and the DNI Office of General Counsel, assesses datasets to determine whether the dataset warrants "enhanced safeguards." This internal determination may be based upon the "sensitivity of the data," "the potential harm or embarrassment to a United States person that could result from improper use or disclosure," or other factors outlined in the guidelines. What "enhanced safeguards" should be provided are determined by the NCTC at its discretion, after taking into consideration requests and recommendations from the data provider.

access to the non-terrorism-inclusive datasets for pattern-based queries in writing, testifying that the dataset is "likely to contain significant terrorism information." Furthermore, the NCTC is subject to numerous checks within the intelligence community itself, such as submitting its internal periodic reviews to various offices and subjecting itself to audits by the Office of the Intelligence Community Inspector General.[21] In addition, the Privacy and Civil Liberties Oversight Board, an independent executive branch agency with authority to analyze and review executive branch actions to combat terrorism, advises the President on the privacy and civil liberties concerns of reviewed actions.

Enhancing Oversight and Enabling Intelligence

While there is no reason to believe that the NCTC would not make limited and appropriate use of this data, it is essential that Congress exercise rigorous and periodic oversight of this process even with these safeguards in place. Indeed, a Reaganesque "trust but verify" approach is appropriate. Of course, it is also vitally important that government officials have access to the information they need to ensure that terrorist acts do not occur. However, given the serious privacy implications and the potential for abuse, it is equally vital that Congress ensure that existing internal and external controls are being followed. In order to do so, Congress and the Administration should:

- **Conduct regular and rigorous oversight hearings to ensure privacy is being protected.** To ensure that the NCTC is respecting the legitimate privacy rights of people living in the United States, Congress should provide effective oversight to verify that the NCTC is using its expanded authority appropriately.

- **Maintain essential counterterrorism and intelligence tools.** Important investigative and intelligence tools, such as the new NCTC guidelines and the PATRIOT Act, are essential to maintaining the security of the U.S. and combating terrorist threats. Indeed, the 2012 NCTC guidelines help to ensure that investigators and analysts can better connect the dots and halt potential terrorists, while key PATRIOT Act provisions, such as the roving surveillance authority and business records provision, have proven essential in thwarting terrorist plots. Preserving and institutionalizing these tools and capabilities are essential to thwarting terrorists before the public is ever put in danger.

- **Establish a national counterterrorism and intelligence framework.** For counterterrorism and broader information sharing to be more effective, each entity and level of government must clearly know its role. The U.S. should designate and delineate the responsibilities of the federal, state, and local governments based on their available resources and ensure that information sharing occurs at all levels. Additionally, the Department of Homeland Security must be better integrated into the counterterrorism and intelligence community and regarded as an equal player. Specifically, Congress and the Obama Administration should consider whether the department should play a more prominent leadership role in the Terrorist Screening Center and the NCTC.

Counterterrorism, Privacy, and Civil Liberties

The 2012 NCTC Guidelines contain important changes that will allow the NCTC to more capably combat domestic terrorist threats. While ensuring that U.S. counterterrorism and intelligence authorities have the tools they need to halt terrorist acts before they occur is important, it is also essential to ensure that any expansion of government data retention and usage is coupled with effective oversight to protect civil liberties and rights to privacy. National security is of the utmost importance, but so is individual liberty.

*—**John G. Malcolm** is a Senior Legal Fellow in the Edwin Meese III Center for Legal & Judicial Studies at The Heritage Foundation. **Jessica Zuckerman** is a Research Associate in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. **Andrew Kloster** is a Legal Fellow in the Meese Center for Legal & Judicial Studies at The Heritage Foundation.*

21. The 2012 Guidelines require the NCTC to provide specific information on privacy-sensitive datasets and office policy for complying with all applicable privacy laws and policies in an annual report, copies of which are provided to the intelligence community element general counsel, civil liberties and/or privacy officer, the NCTC Director, the ODNI General Counsel, and the Office of the Inspector General of the Intelligence Community. While the 2012 Guidelines do not automatically require the NCTC to provide this report to any elected official, it does require the report be made available to the Department of Justice's Assistant Attorney General for the National Security Division upon request. Furthermore, the Intelligence Community Inspector General has authority to audit, investigate, inspect, and review NCTC compliance with privacy law.