Notre Dame Journal of Law, Ethics & Public Policy

Volume 19
Issue 1 *Symposium on Security & Liberty*

Article 10

February 2014

Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence

Michael V. Hayden

BALANCING SECURITY AND LIBERTY: THE CHALLENGE OF SHARING FOREIGN SIGNALS INTELLIGENCE

MICHAEL V. HAYDEN*

Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.
—Benjamin Franklin

While protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right.
—The 9/11 Commission Report[1]

INTRODUCTION

What is the right balance between security and liberty? This question is fixed in the national consciousness as the country faces unprecedented terrorist threats. It is particularly pressing for me as the head of the National Security Agency/Central Security Service ("NSA"),[2] the world's largest collector of foreign signals intelligence. For signals intelligence ("SIGINT"),[3] the current balance was struck in the 1970's as a result of congres-

* Lieutenant General, United States Air Force; Director, National Security Agency; Chief, Central Security Service. President George W. Bush recently appointed General Hayden to serve as the Nation's first Deputy Director of National Intelligence.

1. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 394 (2004) [hereinafter 9/11 COMMISSION REPORT].

2. The National Security Agency ("NSA") is an element within the Department of Defense. NSA is America's cryptologic organization; it coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce signals intelligence. As a high technology organization, NSA is on the leading edge of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the Federal Government. The Director of the NSA is responsible for overseeing the entire United States Signals Intelligence System, which includes the cryptologic elements of the Military Services known as the Central Security Service. For ease of reference, this essay will use "NSA" as an umbrella term for the entire U.S. cryptologic system.

3. Signals intelligence is comprised of communications intelligence and electronics intelligence. Communications intelligence consists of foreign communications passed by radio, wire, or other electromagnetic means. Electronics intelligence consists of foreign electromagnetic radiations such as emissions from a radar system.

sional investigations into activities by NSA and others concerning the privacy of Americans. These investigations led to the creation of the present oversight and legal structure in the executive, legislative, and judicial branches. The events of September 11, 2001, have caused people to assess once again the line between security and liberty. This reassessment manifests itself in a major issue confronting my agency today: how to share SIGINT more broadly while protecting U.S. privacy rights.

I. STRENGTHENING SECURITY: THE IMPERATIVE TO SHARE

A great deal of attention has been paid in the aftermath of 9/11 to the need to share terrorism information more widely. The 9/11 Commission, for example, found that some information about the hijackers was not effectively communicated between federal entities. To rectify this, it recommended that information be shared horizontally, across new decentralized networks that transcended individual agencies.[4] The President's recent Executive Order 13,356 implements this recommendation by promulgating guidelines on the responsibility of federal departments and agencies to share terrorism information and to prepare it for maximum distribution; ordering the development of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States; and establishing an Information Systems Council charged with developing an automated environment for sharing terrorism information.[5] The President also established his Board on Safeguarding Americans' Civil Liberties.[6] On December 17, 2004, the President signed into law the Intelligence Reform and Terrorism Prevention Act of 2004.[7] At the time this article was being prepared, agencies were studying how to implement the Act's provisions creating an "Information Sharing Environment" along the lines recommended in the 9/11 Commission Report.

NSA was already moving aggressively to share more horizontally. Intelligence is not an end in itself. An intelligence agency's main function is to gather the best information available on topics of interest to government clients and pass it to them in a timely and accurate fashion. Intelligence is useful only to the degree that it informs effective action on the part of its users.

4. 9/11 COMMISSION REPORT, *supra* note 1, at 417–18.
5. Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Aug. 27, 2004).
6. Exec. Order No. 13,353, 69 Fed. Reg. 53,585 (Aug. 27, 2004).
7. Pub. L. No. 108-458, 118 Stat. 3638 (2004).

A. *NSA's "Traditional" Approach*

In dealing with the type of SIGINT we call communications intelligence, we have traditionally worked to add value for our clients through a production process encompassing the (1) acquisition of signals, (2) processing of signals into recognizable data, (3) organization of data into knowledge (facts and relationships), and (4) creation of intelligence (applied knowledge). Only in the latter stages of this process have we traditionally published a report to our clients. In dealing with electronic intelligence, a form of SIGINT derived from radar and telemetry signals, we generally have been more comfortable allowing clients to access our system at earlier stages of our production process. This is partly because clients can add their own value to the data, and partly because privacy concerns with this form of SIGINT are minimal.

B. *Increased Sharing*

Today, however, NSA is moving to share more communications-based SIGINT and to do so earlier in the process. Driven by the demands of the war on terrorism, our Intelligence Community partners and clients increasingly want, and need, to "swim upstream" in the production process and take a more active role in the creation of our communications SIGINT products and services.

NSA is making transformational changes in how we share SIGINT with our Intelligence Community partners and clients. This sharing is consistent with Executive Order 13,356, the Director of Central Intelligence's emphasis on greater collaboration, and the Defense Department's work on horizontal integration. NSA has already demonstrated great success in sharing with multiple agencies in Operations Enduring Freedom and Iraqi Freedom. We have pioneered joint, multi-intelligence reporting with Intelligence Community and Department of Defense ("DoD") components, embedded analysts with other intelligence agencies, provided database access and knowledge sharing as part of new partnerships with intelligence agencies, and begun a geospatial analysis training course for joint military and multi-agency personnel.

NSA is willing to provide information in whatever form a client may find useful, and the client's information needs and ability to add value will determine how far up the SIGINT production process he needs to swim. We understand that our clients have a need for certain SIGINT data elements derived from adversary communications. Some clients may even have

the language skills to want the native language content of intercepts and transcripts. NSA is working hard to meet client information needs while maintaining legal obligations regarding U.S. privacy.

II. PRIVACY CONCERNS ABOUT SHARING SIGINT

The 9/11 Commission is absolutely correct in noting that "the privacy of individuals about whom information is shared" must be safeguarded.[8] There are special concerns when it comes to sharing SIGINT.

SIGINT is Electronic Surveillance. Producing SIGINT involves conducting electronic surveillance for foreign intelligence and counterintelligence purposes. In order to satisfy the breadth of the requirements for signals intelligence levied by our military and policymaker clients, NSA conducts electronic surveillance across a wide spectrum of media and in large volumes. We hunt for foreign intelligence on a broad range of topics, including terrorism, weapons proliferation, narcotics, money laundering, political and economic developments, tactical military issues, and arms control.

A key point: even though we do our best to avoid obtaining information about U.S. persons at the front end of our collection process, it is inevitable we will obtain it through incidental, or unintentional, collection. Even if the percentage of U.S. person information NSA incidentally obtains were very small compared to the total volume of communications NSA intercepts, we collect so much information that the amount of U.S. person information incidentally collected would not be insignificant.

A practical example illustrates the issue. In response to a client's stated need for information on terrorism, NSA targets the communications of two suspected foreign terrorists, both communicating overseas. During the exchange, one suspected terrorist raises the issue of a prominent U.S. businessman. NSA was not intentionally targeting the businessman, but it incidentally acquired information about him during the legitimate targeting of two suspected foreign terrorists. The businessman's privacy rights would be infringed if NSA were to distribute his name in an intelligence report across the breadth of the executive branch in an unrestricted fashion. Rules are needed to guide intelligence agencies about the collection, retention, and dissemination of information about individuals with U.S. privacy rights so that these activities pass constitutional muster. The 9/

8. 9/11 COMMISSION REPORT, *supra* note 1, at 394.

11 Commission reached the same conclusion: "[T]he sharing and uses of information must be guided by a set of practical policy guidelines that simultaneously empower and constrain officials, telling them clearly what is and is not permitted."[9]

III. Safeguarding Liberty: Oversight and Law

The 9/11 Commission is also right that increased and more rapid sharing "calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."[10] The American people, by experience and temperament, distrust concentrations of power and government operations conducted in secrecy. NSA is a very powerful, secret agency. To keep the people's trust, NSA must be extremely careful to follow rules that have been laid down by elected representatives in the legislative and executive branches, as well as by the courts. These rules are reflected in a framework of oversight and law.

A. *The Oversight Framework*

In performing its mission, NSA constantly deals with information that must remain confidential so that it can continue to collect foreign intelligence on various subjects that are of vital interest to the nation. Intelligence functions are of necessity conducted in secret, yet the tenets of our democracy require an informed populace and public debate on national issues. The American people must be confident that the power they have entrusted to NSA is not being, and will not be, abused. The resulting tension—between secrecy on one hand and open debate on the other—is best reconciled through rigorous oversight. It serves as a needed check on what has the potential to be an intrusive system of intelligence gathering. The oversight structure, in place now for nearly a quarter of a century, has ensured that the imperatives of national security are consistent with democratic values. United States intelligence today is a highly regulated activity and properly so.

U.S. intelligence was not always so highly regulated. The 1970's were a watershed for the Intelligence Community. Congressional investigating committees led by Senator Frank Church and Congressman Otis Pike found that government agencies, including NSA, had conducted a number of intelligence activities directed against U.S. citizens. This included a mail opening effort and placing certain U.S. persons on surveillance watch

9. *Id.* at 419.
10. *Id.* at 394.

lists. The revelations of these committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving intelligence capabilities. In other words, a concerted effort was made to balance the country's need for foreign intelligence with the need to protect core individual privacy rights.

A wide-ranging, new intelligence oversight structure was constructed. A series of laws and executive orders established oversight procedures and substantive limitations on intelligence activities. In the aftermath of the Church and Pike committees' revelations, Congress passed the Foreign Intelligence Surveillance Act ("FISA"), which created a special court for considering and approving surveillances that occur in the United States and thus have the potential to affect rights guaranteed by the Constitution. The House and Senate each established intelligence oversight committees. President Ford issued an executive order that established for the first time a formal system of intelligence oversight in the executive branch. Oversight mechanisms were established within the Department of Justice and within each intelligence agency. The President also established an independent Intelligence Oversight Board ("IOB"). The result today at NSA is an intelligence gathering system that operates within detailed, constitutionally based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the executive branch, and—through FISA—the judiciary.

1. Legislative Oversight

The appropriations, armed services, and intelligence committees of Congress conduct extensive review of NSA activities. The committees regularly call for detailed briefings on NSA's activities. Committee staffers routinely visit NSA Headquarters and field sites. The intelligence committees also receive formal, semi-annual reports from the Department of Justice concerning NSA's activities under FISA. NSA has in place procedures for its FISA and other activities to ensure that the Agency acts in a manner that protects the privacy rights of U.S. persons. These procedures, as well as any subsequent changes, are reported to the intelligence committees prior to implementation. Further, NSA is legally required to, and does keep the intelligence committees fully and currently informed of all intelligence activities, including any significant anticipated intelligence activity; furnish any information on intelligence activities requested by the committees to carry out their oversight responsibilities; and report to the committees any illegal intelligence activity.

2. Executive Branch Oversight

Within the Executive Office of the President, the Intelligence Oversight Board conducts oversight of intelligence activities. The IOB reports to the President and the Attorney General on any intelligence activities the IOB believes may be unlawful. The IOB also reviews agency Inspector General and General Counsel practices and procedures for discovering and reporting intelligence activities that may be unlawful, as well as conducts any investigations deemed necessary to carry out their functions. Agency procedures for protecting privacy rights are provided to the IOB prior to implementation.

In the Department of Justice, the Office of Intelligence Policy and Review ("OIP&R") reviews compliance with the court-ordered procedures designed to protect the privacy rights of U.S. persons. This office also files semi-annual reports with Congress on electronic surveillance conducted under FISA and is intimately involved with NSA's FISA applications. The Office of Legal Counsel at the Department of Justice as well as OIP&R have been involved in setting the legal standards under which NSA's signals intelligence activities are conducted to ensure that these activities strike an appropriate balance between the country's intelligence needs and individual privacy rights.

In the Department of Defense, the Assistant to the Secretary of Defense (Intelligence Oversight) and the Office of General Counsel are engaged in intelligence oversight of NSA. Within NSA, the Signals Intelligence Directorate's Center for Oversight and Compliance, the Inspector General, the General Counsel, and NSA's Intelligence Oversight Board also conduct oversight of NSA activities. The NSA Office of General Counsel conducts extensive privacy protection and intelligence oversight training for all Agency employees who are involved in collection that implicates privacy rights. NSA also enforces a strict set of audit procedures to ensure compliance with the privacy rules.

3. Judicial Oversight

The Foreign Intelligence Surveillance Court ("FISC") is authorized by FISA to issue court orders for electronic surveillance directed against foreign powers or their agents. In reviewing applications for court orders, FISC judges scrutinize the targets, the methods of surveillance, and the procedures for handling the information collected.

B. *The Legal Framework*

A wide array of statutes and executive branch directives govern NSA's intelligence activities. We scrupulously follow these rules. Electronic surveillance conducted for foreign intelligence purposes is regulated by statutory provisions flowing from FISA and procedures flowing from Executive Order 12,333,[11] which manifest themselves in the form of restrictions applicable to all intelligence collection activities and specific restrictions (Attorney General Procedures) regulating NSA's electronic surveillance activities.

1. Statutory Restriction on Electronic Surveillance in the United States—FISA

Under FISA, NSA may only target communications of a U.S. person[12] in the United States if a federal judge finds probable cause to believe that the U.S. person is an agent of a foreign power. Probable cause exists when facts and circumstances within the applicant's knowledge, and of which he has reasonably trustworthy information, are sufficient to warrant a person of reasonable caution to believe that the proposed target of the surveillance is an agent of a foreign power. Under the statute, a judge may determine a U.S. person to be an agent of a foreign power only if there is information to support a finding that the individual is a spy, terrorist, saboteur, someone who aids or abets them, or who enters the United States under false or fraudulent identity for or on behalf of a foreign power.

All FISA collection is regulated by special procedures approved by the FISA Court and the Attorney General. Since the enactment of FISA in 1978, there have been only a few instances of NSA seeking FISA authorization to target a U.S. person in the United States. In those instances, there was probable cause to believe the individuals were involved in terrorism. With regard to 9/11, the intelligence committees have stated that NSA should work more closely with the FBI to coordinate coverage of communications of any terrorists known to be in the United States.[13] The interception of communications in the United States for

11. Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

12. FISA defines a "United States person" as a U.S. citizen; permanent resident alien; an unincorporated association, a substantial number of members of which are U.S. citizens or permanent resident aliens; or a corporation incorporated in the United States. 50 U.S.C. § 1801(i) (2000).

13. SENATE SELECT COMM. ON INTELLIGENCE & HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMM. ACTIVITIES BEFORE & AFTER THE TERRORIST ATTACKS OF SEPT. 11, 2001, S. REP. NO. 107-351, H. REP. NO. 107-792, at 249 (2002).

domestic security purposes is the proper purview of the FBI. NSA supports the FBI by passing any lead information it obtains regarding terrorist threats against the United States. There was close collaboration prior to 9/11, and it became even closer afterwards.

2. Executive Order 12,333 Restrictions Imposed on All Intelligence Collection Activities

There are certain restrictions imposed by Executive Order 12,333 upon all intelligence collection activities engaged in by executive branch agencies. Intelligence collection must be conducted in a manner "consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded."[14] These include the Fourth Amendment's prohibition against unreasonable searches and seizures. Intelligence collection must not be undertaken to acquire information concerning the domestic activities of U.S. persons.[15] The least intrusive collection techniques feasible must be used in the United States or against U.S. persons located abroad.[16] Finally, agencies in the Intelligence Community are prohibited from having other parties engage in activities forbidden by the Executive Order on their behalf.[17] This means that NSA cannot ask another country to illegally spy on U.S. persons on our behalf, and we do not.

Executive Order 12,333 authorizes NSA to collect, process, and disseminate signals intelligence information for national foreign intelligence (and counterintelligence) purposes and in support of U.S. military operations.[18] NSA is not authorized to collect all electronic communications. NSA is authorized to collect information only for foreign intelligence purposes and to provide it only to authorized government recipients. This means that NSA is not authorized to provide signals intelligence information to private U.S. companies, and we do not do so. Legal proscriptions and the fears of some privacy advocates notwithstanding, as a practical matter, it is not technically possible to collect all electronic communications everywhere in the world on an indiscriminate basis.

---

14. Exec. Order No. 12,333, § 2.1, 3 C.F.R. 210 (1981).
15. *Id.* § 2.3(b), 3 C.F.R. 211.
16. *Id.* § 2.4, 3 C.F.R. 212.
17. *Id.* § 2.12, 3 C.F.R. 214.
18. *Id.* §§ 1.12(b)(3)–(b)(7), 3 C.F.R. 208.

3. Executive Order 12,333 Procedures—Specific Restrictions Imposed on NSA's Collection Techniques

In delegating authority to the Director of NSA in Executive Order 12,333, the President recognized that certain intelligence gathering techniques, such as signals intelligence, are particularly intrusive and must be conducted in a "reasonable" manner to comport with Fourth Amendment and statutory requirements. The Executive Order requires, therefore, that certain written procedures be implemented regulating such techniques. The procedures are designed to protect constitutional and other legal rights and limit the use of information collected to lawful governmental purposes. The Executive Order requires that the head of the agency (i.e., for NSA, the Secretary of Defense) and the Attorney General approve the procedures.

NSA has such procedures in place. The Secretary of Defense and the Attorney General have approved them. They are classified and are appended to DoD Directive 5240.1-R, the DoD regulation which implements Executive Order 12,333. The procedures are incorporated into an NSA Regulation and the substance of the procedures is promulgated throughout the signals intelligence system in a detailed directive, U.S. Signals Intelligence Directive 18, signed by the Director of NSA. This Directive provides a single document in which all the restrictions, whether originating from constitutional, statutory, executive order, or regulatory provisions, may be found.

4. Executive Order 12,333 Restrictions on Electronic Surveillance Outside the United States

Under Executive Order 12,333 and implementing regulations signed by the Secretary of Defense and approved by the Attorney General, NSA must obtain the Attorney General's approval before conducting electronic surveillance directed against a U.S. person abroad. The Attorney General must have probable cause to believe that the person is an agent of a foreign power, either an officer or employee of a foreign power, or a spy, terrorist, saboteur, or someone who aides or abets them. Occasionally, NSA seeks Attorney General authorization to target a U.S. person overseas. An example of such a request would be one seeking authorization to target a terrorist overseas who is a U.S. permanent resident alien.

5. Executive Order 12,333 Restrictions Relative To Retention and Dissemination of Unintentionally Acquired U.S. Person Information

NSA's collection of foreign intelligence from foreign individuals and entities is designed to minimize the incidental or unintentional, collection of communications to, from, or about U.S. persons. When NSA does acquire information about a U.S. person, NSA's reporting does not disclose that person's identity, and NSA will only do so upon a specific request that meets the standard derived from statute and imposed by executive order regulation—that is, the information is necessary to understand a particular piece of foreign intelligence or assess its importance. Specifically, no information to, from, or about a U.S. person may be retained unless the information is necessary to understand a particular piece of foreign intelligence or assess its importance. Similarly, no identities of U.S. persons may be disseminated (that is, transmitted to another government department or agency) by NSA unless doing so is necessary to understand a particular piece of foreign intelligence or assess its importance. For example, if NSA intercepted a communication indicating that a terrorist was about to harm a U.S. person, the name of the U.S. person would be retained and disseminated to appropriate law enforcement officials.

IV. SHARING SIGINT TODAY AND TOMORROW

A key question in the debate about balancing security and liberty is whether information related to terrorism can be more effectively used to protect national and homeland security in a manner consistent with the current statutory and constitutional protections afforded to U.S. citizens. The answer is "yes." SIGINT on terrorism can be effectively shared within the current oversight and legal framework. Improvements can and will be made in how NSA shares SIGINT, but these issues are primarily policy questions, not legal ones. The current framework is sufficiently flexible to accommodate the changes that need to be made.

For example, Executive Order 12,333 establishes the legal requirement that persons granted access to SIGINT databases likely to contain U.S. person information be made aware of the privacy considerations involved in handling material produced by sensitive electronic searches and be trained in the proper procedures to handle such information. Intelligence analysts from any agency can be trained in this area, and NSA is doing so. The real challenge is the policy one of establishing and maintaining

oversight of the sharing process to ensure Fourth Amendment-compliant procedures are being followed. As head of the U.S. SIGINT system, I am responsible for the lawfulness of that system and need to have confidence in the compliance of agencies that have been granted access to sensitive SIGINT data.

We must also ensure that sharing initiatives actually promote efficiency and effectiveness. Again, this is not a legal issue. Stewardship of public funds demands that inefficient use of resources be avoided. No one would be well served by unfounded analytic judgments published by analysts lacking the experience to handle the data provided. Specialization carries benefits in intelligence, as in medicine and other fields of endeavor. We must focus our efforts to share upon those who can truly act on or have the expertise to add value to what we can provide.

To use a sports analogy, we need to "play position." Like a major league soccer team, we need players (i.e., agencies) who can utilize their unique and considerable talents at each position to work together in a coordinated fashion for the common goal of national security. There are certain skills agencies have developed over the years that enable them to provide valuable services to clients, including substantive knowledge about the target. The country needs to find a smart way to share SIGINT that allows each party to use its strengths.

Perhaps the greatest challenge in sharing is "connecting the dots" across departments and agencies when the dots appear insignificant on their own. After processing the data they collect, intelligence agencies report information to fulfill client requirements in accordance with established priorities and thresholds. Each agency is left with unreported data and information that do not appear to be of intelligence value and are well below anyone's reporting thresholds. If such data points of SIGINT were married up with the data points of human intelligence, imagery, or law enforcement information, perhaps we would end up with information of high value to national security. We have to determine how we can create such linkages without fostering chaos regarding Fourth Amendment protections. The procedures required by Executive Order 12,333 to protect U.S. privacy rights have worked well for many years by preventing abuses and should serve as the model when expanding information sharing on terrorism.

While working to improve sharing, we need to keep fundamental security concerns with regard to sources and methods firmly in mind. No matter how far upstream clients may swim in the intelligence production process, each intelligence agency has

data that it is obliged to protect in order to ensure its continued ability to produce intelligence to serve those very clients.

There have been some special concerns raised about sharing SIGINT with law enforcement. Much has been said in recent congressional hearings and the 9/11 Commission Report about a "wall" between intelligence and law enforcement. I will speak only of NSA but I think it fair to say that, historically, we have been able to be more agile in sharing information with some clients (like the Department of Defense) than we have with others (like the Department of Justice). This is not something that we created or chose. For very legitimate reasons, Congress, the executive branch, and the courts erected some barriers that made sharing with law enforcement more careful, more regulated. We chose as a people before the attacks of September 11, 2001, to make it harder to conduct electronic searches for a law enforcement purpose than for a foreign intelligence purpose. This was so because law enforcement electronic searches implicate not only Fourth Amendment privacy interests, but also Fifth Amendment liberty interests. After all, the purpose of traditional law enforcement activity is to put criminals behind bars. The purpose of traditional foreign intelligence activity, in contrast, is to protect the country from foreign threats.

With the passage of the USA Patriot Act after 9/11 and a recent decision by the FISA appellate court lowering "the wall," the line has been redrawn.[19] More information is flowing between NSA and law enforcement agencies. By changing the "purpose test," the Patriot Act made it easier for law enforcement agencies to get approval from the FISA Court for foreign intelligence surveillance. Prior to the Patriot Act, the FISA required that the executive branch had to certify to the court that "the" purpose of the surveillance was to obtain foreign intelligence information.[20] Section 218 of the Patriot Act amended the law by requiring that the executive branch had to certify only that "a significant" purpose of the surveillance is to obtain foreign intelligence.[21] Thus, purposes beyond foreign intelligence (i.e., criminal matters) may be served under the new formulation. This clarifies any ambiguity about when FISA Court approval is appropriate in cases, such as terrorism, that can be both foreign intelligence and criminal matters. In addition, the Patriot Act clarified

19. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter Patriot Act]; *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

20. 50 U.S.C. § 1804(a)(7)(B) (2000).

21. Patriot Act § 218, 115 Stat. at 291.

that law enforcement agencies may pass information obtained in criminal matters to intelligence agencies.[22] The Patriot Act is an important tool in fighting terrorism because it promotes information sharing in a regulated way.

The successful balancing of intelligence activities and privacy protection requires effective oversight; yet, the 9/11 Commission has called congressional oversight of intelligence "dysfunctional."[23] The current oversight structure has worked in at least one regard: the privacy issues uncovered in the 1970's have not returned and quality SIGINT continues to be produced. The process of reporting to legislative, executive, and judicial bodies has created a culture at NSA that respects the law and the need to protect U.S. privacy rights. Through training and job oversight mechanisms, this "culture of compliance" gets passed down to succeeding generations of employees. NSA is able to accomplish its mission within a culture of compliance, and this will continue.

CONCLUSION

In the post-9/11 environment, the nation is debating how to balance security and liberty. The 9/11 Commission has called for rules with oversight to protect privacy when expanding information sharing on terrorism. The President responded with a new executive order to promote increased sharing of terrorism information and by signing the Intelligence Reform and Terrorism Prevention Act. A set of rules, along with an oversight structure, has prevented government abuse of SIGINT for nearly a quarter of a century. Terrorism information may be shared more broadly today under this framework, suggesting that this is not a zero-sum game. That is, expanding the sharing of signals intelligence, under the law and in accordance with effective oversight by the executive, legislative, and judicial branches, can strengthen security without diminishing the constitutional liberties of the American people.

22. *Id.* § 203, 115 Stat. at 278–81.
23. 9/11 COMMISSION REPORT, *supra* note 1, at 420.