Heritage Lectures
Published by The Heritage Foundation

No. 851
Delivered June 25, 2004

September 30, 2004

Information Oversight: Practical Lessons from Foreign Intelligence

Joel F. Brenner

Lytton Strachey announced in 1918, only half in jest, that the "history of the Victorian Age will never be written." We knew too much about it—so much about it, Strachey thought, that even Edward Gibbon, who charted *The Decline and Fall of the Roman Empire,* could not have got his arms around it. In the face of this information glut, Strachey's strategy in writing *Eminent Victorians* was to "row out over that great ocean of material, and lower down into it, here and there, a little bucket, which will bring up to the light of day some characteristic specimen, from those far depths, to be examined with careful curiosity."

Strachey didn't know the half of it. Intelligence agencies in the United States have long had the same predicament Strachey diagnosed so acutely, but without the historian's luxury of intervening years to figure out where to dip the bucket. Meanwhile, the size of the ocean has grown by many orders of magnitude. Every year Internet traffic doubles.[1] Every week 630,000 telephone lines are installed in the U.S. alone.[2] Every day 50,000 wireless subscribers join 18 million existing subscribers in the U.S. alone.[3] Every hour 674,000 international phone calls are made from the U.S.[4] Every minute 21.5 million e-mails are sent.[5]

The implications of this data[6] glut for a democracy are stark: What information should we permit the government to gather and disseminate about its citizens? Should the same rules apply to the private sector? And however these questions may be answered, how do we give the public reasonable assurances that the rules are

This article explores the implications of the growing electronic data glut on democratic institutions and notes that the National Security Agency has years of practical experience in the supervision of complex systems for gathering and protecting information. The author argues that the evolution of NSA and its oversight structures offer useful lessons to those grappling with the balance between privacy and security, and proposes ten practical principles that should be applied to the human and the technical aspects of information systems.

* * *

This article is published simultaneously by The Heritage Foundation and the Center for Democracy and Technology. The views expressed are those of the author and do not necessarily reflect the official policy of the National Security Agency, the Department of Defense, or the U.S. Government. The author is grateful to the McCormick Tribune Foundation and the National Strategy Forum for their sponsorship in June 2004 of the Cantigny Conference on "Counterterrorism, Technology and Privacy," which stimulated this article.

This paper, in its entirety, can be found at:
www.heritage.org/research/nationalsecurity/hl851.cfm

Produced by the Center for Legal and Judicial Studies
and the Center for Democracy and Technology

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

being obeyed? Several recommendations of the 9/11 Commission now place this last question in immediate relief. Specifically, the commission recommended that as the President determines guidelines for information sharing among government agencies and with the private sector, he should safeguard information about private citizens; that a board be established within the executive branch to oversee the guidelines and protect civil liberties; and that Congress should address the "dysfunctional" state of its own intelligence oversight.[7] The National Security Agency (NSA) has years of practical experience in the supervision of some of the world's most complex systems for gathering, processing, disseminating, and protecting information. The evolution of NSA and its internal and external oversight structures offer useful lessons to those grappling with these issues.

NSA manages the nation's foreign signals intelligence, or "SIGINT." SIGINT includes communications intelligence—the transmission of voice and data, for example. It also includes signals from the launch or trajectory of a missile or the characteristics of foreign radar systems. Since many signals are encrypted, code making and code breaking have always been an important part of the Agency's work. But the Agency was not created on the Seventh Day. It grew from years of difficulty and experience.

Some NSA History

NSA evolved from American cryptanalytic work that had proceeded in fits and starts following World War I. American entry into that war was actually accelerated by the pioneering cryptanalytic efforts of the British, who intercepted and decoded the famous "Zimmerman telegram" that disclosed German efforts to enlist Mexico in war against the United States.[8] British tutelage was also critical after the war in encouraging fledgling American efforts at code making and breaking, and a super-secret group in the State Department called the Cipher Bureau, a.k.a. the Black Chamber, began breaking Japanese diplomatic codes as early as 1919. Unfortunately, the Black Chamber was abruptly shut down in 1930 by President Hoover's Secretary of State, Henry L. Stimson, who is chiefly, if unfairly, remembered (if at all) for his quaint remark that "gentlemen do not read each other's mail."[9] Thereafter, the work of de-coding and de-ciphering[10] continued, sometimes in violation of

[1] Andrew M. Odlyzko, "*Internet Traffic Growth: Sources and Implications*," paper for the University of Minnesota Digital Technology Center, (2003), p. 1.

[2] Extrapolated from Federal Communications Commission, Press Release: "Federal Communications Commission Releases Study on Telephone Trends," May 6, 2004, p. 1, referring to 16.3 million lines installed in the six months before June 30, 2003.

[3] Extrapolated from *ibid*., p. 11-3, referring to about 18 million total subscribers increasing by 49,315 subscribers in the 12 months before December 2003.

[4] Extrapolated from *ibid*., p. 6-1, referring to 5.9 billion such calls in 2002 (the most recent year for which such data were available from the FCC).

[5] Extrapolated from Google, search question posted March 1, 2004 (Question ID # 312337), referring to 31 billion e-mails daily.

[6] It is important in many contexts to clarify whether one uses words such as "data," "information," and "raw traffic" to refer to ones and zeroes, encrypted text, plain text, or a distilled synthesis of fact and judgments. But those distinctions are not material here. At every level the volume, velocity, and variety have exploded.

[7] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Co., 2004), pp. 394, 395, and 420, respectively.

[8] Barbara Tuchman, *The Zimmerman Telegram* (New York: Ballantine Books, 1966).

[9] G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly Press, 1991), pp. 328–335; see David F. Schmitz, *Henry L. Stimson: The First Wise Man* (Wilmington: Scholarly Resources Books, 2001).

[10] A code involves substituting words, numbers, or other symbols for words in plain text. A cipher involves substituting words, numbers, or other symbols for the letters of a plain text message. Ciphers are more complex and nowadays typically require powerful computers to make or break. Encryption may refer to either encoding or enciphering.

law, chiefly in the Army's Signals Intelligence Service (SIS) and the Office of Naval Communications, and in 1940 the SIS finally broke the most difficult of the Japanese naval ciphers, dubbed "Purple."[11] This was the breakthrough that enabled Admiral Chester W. Nimitz to ambush the much larger Japanese fleet at Midway in 1942.

After the war, however, there was no organizational framework for putting such skills at the service of the whole national government. In 1947, Congress created the Department of Defense, the National Security Council, and the Central Intelligence Agency (CIA), but signals intelligence remained separately imbedded in the various armed services. So in 1949, the Defense Secretary created the Armed Forces Security Agency (AFSA). AFSA reported to the Joint Chiefs, however, which meant that SIGINT remained a military, rather than a national, intelligence function. And AFSA required unanimous agreement to act, which meant that it rarely did. So on October 24, 1952, President Truman issued the top secret order that created NSA. He aligned the Agency directly under the Secretary of Defense, which left the Secretary (rather than the Joint Chiefs) in charge of its budget, but he put NSA policy under the guidance of the Director of Central Intelligence. In this way, both military and non-military interests could be reflected in NSA's choice of foreign intelligence targets.

In 1971, the NSA Director was put in charge of coordinating the collection of SIGINT at the theater and tactical levels for the military. In this capacity the Director functions as the Chief of the Central Security Service. This is basically how the organization stands today.

NSA's contributions to the intelligence effort against the Soviet Bloc were extraordinary,[12] but by 1991 the Agency had been focused for 40 years on an adversary that was slow-footed, technologically backward, and rigidly organized. Then the Soviet Bloc collapsed, and many fondly hoped that we were entering a strife-free age when threats to the nation's security had vanished. Instead, we began reaping a harvest of conflicts that had been suppressed since, depending on your view, 1945 or 1919. Meanwhile, a wave of technological innovation began flooding the world with powerful, tiny communications devices that were hardly imaginable a short time earlier. In 1991, NSA was passively pulling analog signals out of the air—and the Agency was very, very good at it.

By 2001, NSA faced myriad adversaries that were unlike the Soviets: They were quick afoot, technologically shrewd, and loosely organized. Moreover, a decade of under-funding and, in the view of some critics, indifferent management during the 1990s had left the Agency behind the curve. The volume and velocity of communications were staggering; even the variety of targets was staggering. NSA therefore began a belated shift from the discrete circuit communications used during the Cold War—mostly analog technologies like high-frequency voice, VHF tactical voice, line-of-sight microwave, and satellite communications—to an encrypted global network of public internets, extranets, and supranets, some of them wireless, all of them digital, that virtually connect the world. This evolving global grid is increasingly connected by high-capacity fiber-optic backbones that convey digital packet-switched data to provide multimedia services that in turn create insatiable demand for bandwidth. At the same time, strong encryption that was formerly available only to governments became available to every kid with a PC.

And so we are back to Strachey's dilemma: You must know where to dip the bucket. Gathering all the bits of data floating around in the hope that you can sort through it all—in effect, swallowing the sea—is a fatuous idea. No organization, and no technology, can do it. Doing SIGINT for foreign intelligence purposes therefore implies electronic filtering, sorting, and dissemination systems of amazing sophistication, but that are imperfect.

[11] O'Toole, *Honorable Treachery.*, pp. 336–345. "Purple" used both a code and a cipher. *Ibid.* For the comparable story in the European theatre, see David Kahn, *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943* (Boston: Houghton Mifflin Co., 1991).

[12] For unclassified portions of this history, see *www.nsa.gov/cch/index.cfm*.

Nor does the problem end here. Once you gather data, you must decrypt it, translate it, analyze it to make sense of it, sanitize it to protect the sources and methods of collection, and route it—or parts of it—to the people who need to know it. Routing, or dissemination, is itself an enormously complex problem, and the government did not do well on this score.

While NSA does not disseminate information outside intelligence and military channels, it has made great strides in producing intelligence that can be widely disseminated without compromising sources and methods, while also imposing appropriate levels of security at different levels of disclosure. The eventual level of disclosure may be the mayor of Los Angeles, the head of a regional transportation authority, or a battalion commander in Iraq. This is happening almost seamlessly on the military side, and it has begun to happen regularly, if imperfectly, on the civilian side.

The challenge now is aligning the technologies and database architectures of the many military and civilian organizations and agencies that produce or consume sensitive information at the federal, state, and local levels. Doing this right will require more time and more money, lots of it; and the task will never be finished because the technology is changing constantly. Like most difficult problems, this one has no permanent solution. The best we can hope for, and the least we should expect, is that it be managed reasonably well.

Managing information also has a defensive side: You have to keep it from people who want to steal it, hackers as well as spies. As recently as the 1980s, NSA was basically a big ear. The model was: They transmit, we listen. The Agency also devised codes, but it operated essentially on a garrison model, as if surrounded by a moat. Two things changed that. First, before the 1980s few people knew NSA even existed. We were "No Such Agency." Now everybody knows that we listen, and that makes our job harder. Our operations have therefore become far more agile and less concentric. Second, now that the world is linked, NSA is transmitting all the time—moving, routing, sorting information. This means NSA is a target. Others are constantly hunting, hacking, and disrupting the Agency—or trying to do so. As a result, the current Director, Air Force Lt. Gen. Michael V. Hayden, elevated the importance of the Agency's defensive or "information assurance" operations when he reorganized the Agency in 2001.

An organization charged with gathering, protecting, and disseminating information faces the most difficult issues that a governmental body has to contend with: Its structures as well as its technologies must be fluid. It must have the funds to develop and implement, or adopt and implement, technology at least as fast as the private sector, and it must have efficient mechanisms for deciding how to spend that money effectively. By the end of the century, NSA's inability to manage its acquisition process was probably its greatest weakness, and although the Agency under Director Hayden has made significant progress in addressing that weakness, the task is not finished. Issues like this—organizational structure, technological agility, and acquisition skills—hold little public interest, but they are essential to the Agency's ability to do what the public does demand that it do well, which is to keep it safe and to operate secretly but under the law.

Secrecy in an Open Society

NSA operates in secret on behalf of a democratic republic that is deeply and properly distrustful of secrecy. The conduct of such a mission is tolerable only when it is performed in conformity with the laws and lawful orders of elected officials, and in the long run, only when the agencies that do it enjoy the nation's trust—trust in their competence and trust in their integrity. NSA has a foreign, not a domestic, intelligence mission, and this restriction is deeply ingrained in the Agency's leadership and workforce. The only time NSA may target the communications of a United States person[13] in the United States is when there are reasonable grounds to believe such a person, acting on behalf of a foreign power, is knowingly engaging in, or is aiding or abetting, espionage, sabotage, or terrorism. And even then, there are laws and orders that dictate how the Agency must go about it. According to the Joint Congressional 9/11 Report, "Joint Inquiry interviews of a wide range of NSA personnel, from the Director down to analysts, revealed the consistent theme that NSA did not target individuals in the United States."[14] That an intelligence agency should be singled out—even criticized—for its "cautious approach to any collection of intelligence in the United States"[15] is an extraordinary turn of events.

It was not always so. Most of the laws, orders, and organizational changes that affect NSA's operations were put in place as a direct result of the spy scandals and resulting congressional investigations by the Church and Pike Committees in 1976.[16] These investigations disclosed widespread abuses by the intelligence agencies, generally at the request of the executive. Most of them did not involve NSA, but some did—including spying on U.S. citizens for political purposes. As a result of that scandal the pressure for reform was intense, and in 1978 Congress passed the Foreign Intelligence Surveillance Act (FISA). That Act established a special court to hear applications for warrants permitting the interception of communications of specific U.S. persons within this country where there is probable cause to believe they are engaging in, or are aiding and abetting, espionage, sabotage, or terrorism on behalf of a foreign power. If the U.S. person is abroad, the Attorney General may authorize the collection under Executive Order 12333.

Sometimes NSA unintentionally acquires information to, from, or about U.S. persons in the course of targeting a foreign person abroad. Such incidentally acquired information may be retained and disseminated only under narrow circumstances. The information must satisfy a foreign intelligence requirement, and the identity of the U.S. person may be disseminated only if the identity is necessary to understand the foreign intelligence or assess its importance. NSA's Inspector General reports quarterly on all violations of these rules, whether intentional or accidental, to the chairman of the President's Intelligence Oversight Board. These reports not only serve an important external monitoring function; they also have a useful deterrent effect, because mistakes have to be explained, and no one likes to do that.

Oversight Structures

In 1976, the Senate established the Select Committee on Intelligence to provide legislative oversight of the intelligence community. A year later, the House followed suit and set up the Permanent Select Committee on Intelligence. These committees play an active oversight role and their significance can hardly be overstated—even if their composition, rules, and focus will inevitably be the subject of debate from time to time (as they are now).[17] In effect, they are the clutch that permits two otherwise conflicting imperatives of two great branches of government to work more or less in synch: on the one hand, the executive's demand for a reasonable degree of secrecy in the conduct of

[13] "'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section." Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1801(i). NSA also monitors the security of communications of various government entities, usually military—but only on request of the entity.

[14] *Joint Congressional Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, S. Rep. No. 107-351, H.R. Rep. No. 107-792, December 2002, p. 74.

[15] *Ibid.*, p. 72.

[16] See *Intelligence Activities and the Rights of Americans, Book II, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities Together with Additional, Supplemental, and Separate Views*, S. Rep. No. 755, 94th Cong., 2d Sess. (1976) ("Church Committee Reports"); *Recommendations of the Final Report of the House Select Committee on Intelligence*, H.R. Rep. 833, 94th Cong., 2d Sess. (1976) ("Pike Committee Reports"). The Church Committee Reports, but not the Pike Committee Reports, were made public, but the latter were eventually leaked, and both sets of reports, comprising many volumes, are available online. See also L. Britt Snider, "Recollections from the Church Committee's Investigations of NSA," *Studies in Intelligence* (Winter 1999–2000), at *http://intellit.muskingum.edu/cia_folder/cia70s_ folder/cia70sinva-l.html*.

[17] See, *e.g.*, *Final Report of the National Commission on Terrorist Attacks,* pp. 394–395.

sensitive affairs, and on the other, the legislature's demand for information about significant government operations and the uses to which appropriated funds are put. Before 1976 these imperatives seemed frequently irreconcilable; one or the other (usually disclosure) was often sacrificed—or else the disclosure was handled in a private, off-the-record exchange with a powerful legislator.[18] Releasing classified information to 535 members of Congress, and inevitably to their staffs, would create an unacceptable risk of disclosure. This was usually the executive's reason for keeping Congress in the dark. The Intelligence Committees now provide a way of dealing with this conundrum without either side's feeling its gears have been stripped. Depending on the sensitivity of particular disclosures, the executive releases classified information either to the chairmen and ranking members of the two committees, or to the entire committees—but not to the entire Congress. Regardless of your view of whether this arrangement can be improved, it solves a fundamental problem. It also addresses the corrosive effect of secrecy: as Frederick Hitz recently paraphrased Lord Acton, "absolute secrecy corrupts absolutely."[19] The Intelligence Committees removed the excuse for absolute secrecy.

The first executive order establishing general ground rules for the intelligence agencies was issued by President Gerald Ford in 1976.[20] With minor changes, a similar order remains in effect today as Executive Order 12333, issued by President Ronald Reagan in 1981. This order limits NSA's mission to the collection, processing, retention, and dissemination of signals intelligence information for foreign intelligence purposes, and it requires NSA—and all our intelligence agencies—to use the least intrusive collection techniques feasible within the United States and against U.S. persons abroad. NSA's surveillance procedures must be established by the Secretary of Defense and approved by the Attorney General. NSA's procedures are also vetted by the Intelligence Committees and, in the case of FISA surveillances, by the FISA Court.

There are numerous additional layers of oversight within the executive branch itself. The Justice Department engages in broad oversight of NSA's policies through its Office of Intelligence Policy and Review, as does the President's Foreign Intelligence Advisory Board. The Assistant to the Secretary of Defense for Intelligence Oversight is further empowered to review activities as well as policies throughout the intelligence community. And the Inspector General of the Department of Defense is empowered to review any aspect of that Department, including the operations of the Defense Agencies, of which NSA is one. As a practical matter, however, NSA's Inspector General conducts the most intense and effective executive oversight of NSA's operations.[21] In that capacity I have broad authority to audit, investigate, and inspect virtually

[18] See, *e.g.*, Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003), p. 446, presenting the views of Judge Griffin Bell of Atlanta, who was Attorney General under President Jimmy Carter, on how Helms's disclosure dilemma would have been handled if Senator Richard Russell of Georgia had still been in the Senate.

[19] Frederick P. Hitz, *The Great Game: The Myth and Reality of Intelligence* (New York: Alfred A. Knopf, 2004), p. 127.

[20] Ex. Ord. 11905, "United States Foreign Intelligence Activities," February 18, 1976, 41 F.R. 7703, *superseded by* President Jimmy Carter's Executive Order, Ex. Ord. 12035, same title, January 24, 1978, 43 F.R. 3674, *superseded by* President Ronald Reagan's still current Executive Order, Ex. Ord. 12333, "United States Intelligence Activities," December 4, 1981, 46 F.R. 59941.

[21] The Department's Inspector General (IG) is a creature of statute, the Inspector General Act of 1978, Pub. L. 95-452, 92 Stat. 1101. The Act's numerous amendments are codified at 50 U.S.C.—App. and are available online at *www.ignet.gov/*. In contrast, the NSA IG is a creature of Agency regulation, NSA/CSS Directive 10-4, November 26, 1997, promulgated by then Director Vice Admiral Michael McConnell. The Agency had had an IG since its beginning, but the IG had no audit staff until 1990, when the Intelligence Committees mandated such an audit function. The IG position was filled with a senior career civil servant until 1996, when Admiral McConnell adopted the practice, followed by General Hayden, of appointing an IG from outside the Agency.

any activity in the Agency, and I exercise that authority through a competent and experienced staff of more than 60 professionals and support personnel. Our collective experience in conducting oversight of a large, far-flung, and technically sophisticated intelligence agency may have something to teach legislators and policy-makers contemplating an expanded role for domestic antiterrorism activities. I will not enter here into the debate over the wisdom or necessity of such activities; but to the extent that they may be done, they should be done well—and scrupulously according to law.

Conducting Effective Oversight

Intelligence is a regulated industry. To be sure, it is not just *any* regulated industry. Both its practitioners and the general public are aware that intelligence is special, in a world of its own. But it is a regulated industry nonetheless, and it presents one troublesome problem in common with other regulated industries. And that is, that getting a large regulated bureaucracy to behave itself, and finding out whether it actually is behaving itself, is a difficult business. This is true whether you are overseeing the activities of covert agents, supervising the tasking of communications intercepts, or monitoring the activities of brokers on the phone with their clients or trading on the floor of a securities exchange. In fact, devising systems to find out whether someone is illegally eavesdropping on U.S. citizens is not that different from devising systems to find out whether brokers are trading their own interests ahead of their customers' interests.

Which leads to the first of ten principles that are basic to the establishment and maintenance of a robust and reliable system of oversight, particularly of information systems that support intelligence. They are not comprehensive, and they are consistent with the thoughtful and useful auditing guidance by the Government Accountability Office (formerly the General Accounting Office) and the Office of Management and Budget.[22] The first four principles address the human characteristics of effective oversight; the next six address technical characteristics.

Principle No. 1: *A culture of compliance is every organization's—and the public's—best safeguard against misbehavior, and no amount of effort to create and sustain that culture is too great.*

Regardless of the technology, no oversight system will prove robust and reliable if it is not managed by capable people who believe in their mission. Those of us who work in this area—lawyers counseling clients, inspectors general, compliance officials in every kind of business—know what others are sometimes surprised to hear: that a conscientious, well-trained workforce, indoctrinated in law and policy, is the most important defense against misbehavior. Without such a workforce, any system of laws and regulations can be subverted. Corporate culture is what auditors call the control environment. It is critical because the level of quality that can be inspected or policed into any system is quite limited, and this is true whether you produce automobiles, SIGINT, or anything else. You can inspect or police for flaws and violations, but you will never catch them all. Quality must be built in, not layered on; and people do that, not machines. In this respect, NSA's workforce is superb.

A culture of compliance starts from the top and will not be created or sustained without continual support from the top. Organizations reflect the styles and values of those who lead them. The rhetoric of leadership is important, but people watch what their leaders do: watch the budgetary and operational decisions that reflect what their leaders really think and want. If the chairman, president, or director exhorts the workforce to take intelligent risks but cuts programs that fail to produce short-term results, everyone gets the real message. If the CEO tells the sales force they are fiduciaries for their customers but offers big incentives to sell the company's proprietary investment products that have lower returns than competing products and may be unsuitable for many customers, the brokers get that message too.

[22] See General Accounting Office (GAO), *Standards for Internal Control in the Federal Government* (the Green Book), November 1999; GAO, *Government Auditing Standards* (2003 Rev.); OMB Bulletin 01-02, "Guidance on Performing Audits of Federal Agencies," among others.

Similarly, if an intelligence agency forbids the interception of certain communications and backs that up by punishing any violator—which is what happens at NSA—the workforce knows that the rhetorical message is the real one. There are bad actors in every large organization. The difference between good and bad organizations is whether bad actors thrive in them, or whether they are cut out like cancer, the earlier the better. Carrying out this policy requires that expectations regarding behavior be clear, which leads to the next principle:

Principle No. 2: *Every significant function in the system should be regulated by unambiguous written procedures.*

Oversight and compliance officials sometimes need to remind management of three reasons why written procedures help managers be more effective. First, they are inseparable from the training function. There are right and wrong ways, better and worse ways, and lawful and unlawful ways of running a business. Procedures are essential to train employees in the organization's way of doing things. Second, procedures are the standard to which you hold people accountable. And third, procedures help discipline managers who know what they're doing but can't manage. We've all seen the old hand who really does know better than anyone else how a certain aspect of the business works but who has it all in his head; who resists attempts to change his ways; and who hasn't got the sense to hire a deputy or assistant who has the organizational strengths to complement his own weaknesses. Under this kind of manager, consistent policy is difficult to establish and police, liaison with the rest of the business often suffers, and continuity gets lost. And when this person gets sick, goes on vacation, or retires, his end of the business falls apart.

I emphasize, however, that only significant functions require procedures. Procedures are not ends in themselves. Unfortunately, every large organization nowadays seems to spawn a group of people who act as if the organization's principal product is process. This fundamental misconception thrives among employees in non-production functions, including compliance and oversight, because it tends to support the need for what they do. Production managers resent this point of view as a drag on the business—and they're right. Process exists to serve production or other objectives imposed by management or regulation, and the leader of a compliance or oversight group who wants to retain credibility with management had better understand this. If a procedure isn't necessary to assure safety or one of the key functions I mentioned—training, accountability, policy consistency, continuity, and liaison—it's pointless or worse.

A similar note of caution concerns enforcement. In the absence of discretion, any set of rules can degenerate easily into tyranny or foolishness. This is why the Justice Department promulgates "Principles of Federal Prosecution" to promote "the reasoned exercise of prosecutorial discretion" in determining "when, whom, how, *and even whether* to prosecute for apparent violations of Federal criminal law."[23] If discretion is appropriate in the enforcement of federal criminal law, it is also appropriate in the enforcement of agency regulations. Some violations are too trivial to bother with. Others should be excused so we can get on with the real work. Some require a prompt and severe response. Yet surprisingly, the notion of discretion sits uneasily with some members of the federal inspector general community, with whom the reflexive devotion of investigative resources to every complaint that sails over the transom can become a habit. Discretion is an inescapable function for any oversight official seriously interested in controlling his organization's resources and managing risk. Just as NSA SIGINT managers must make decisions about where to dip their buckets, so must oversight managers make decisions about where to devote resources to address the greatest risks of fraud, waste, abuse, and mismanagement.

Principle No. 3: *Training in these procedures, and in their reasons for being, should be mandatory, rigorous, lively, and periodically repeated.*

[23] *Principles of Federal Prosecution*, U.S. Department of Justice, *U.S. Attorneys' Manual*, Title 9, § 9-27.110 (emphasis added), available at *www.usdoj.gov/usao/eousa/foia_reading room/ usam/title9/27mcrm.htm*.

At NSA the Office of the Inspector General works closely with the General Counsel's Office and internal compliance groups that train thousands of employees in the restrictions on what our Agency can do. The Agency spends millions doing this, which is why the congressional 9/11 Commission was able to conclude that people at NSA "from the Director down to analysts" play by the rules.[24]

Still, we can do better. Last year, when I was inspecting an NSA facility thousands of miles from Washington, I was asked to speak to a group whose job is to train Agency employees in far-flung locations. How are we doing, I asked, in training our people in the rules governing improper eavesdropping? The response was almost unanimous: We do it, but it's boring. And nobody understands why we do it—even the trainers didn't understand it. This should not have surprised me. Those of us who were adults in the 1970s know in our bones why we have these rules. We saw officials running amok, spying on Americans, and lying under oath, and we remember the necessary but bitter medicine and the long-term damage done to the quality of American intelligence in the scandal's aftermath. Twenty-year-old corporals and techno-geeks know nothing of that history. This is why training must be lively as well as mandatory and rigorous. At NSA, we are working to fix this.

Principle No. 4: *Compliance is an aspect of operations—not a separate oversight function. In contrast, oversight is a separate activity from both operations and compliance, and the office that carries it out must be independent of management. To be effective, both oversight and compliance should be driven by rigorous and frequent risk assessments.*

These are basic tenets of organizational responsibility. Even if you create an office of compliance within an operational component, as NSA does, compliance is the responsibility of operational managers. Compliance is an aspect of quality, and the quality monkey must remain on management's back. The distinction between compliance and oversight therefore reflects the difference between building quality into a product and inspecting for flaws after the fact, which must be done by people who do not report to production managers. Finally, there are never enough resources to review every aspect of any complex business. Choices based on careful risk assessments must be regularly made and frequently re-examined, failures must be anticipated, and new kinds of failures must be imagined and guarded against.

Principle No. 5: *Everything that can reliably be done automatically should be done automatically.*

Technology is essential to address two fundamental problems of any oversight system: reliability and volume. Computers are fast, they don't make mistakes, and they don't get sleepy after lunch. But technology alone never assures anything. Someone always has to decide when and how to implement it. Consider this apparent paradox: NSA spends billions on technology, but when it comes to preventing the dissemination of U.S. person information, we don't rely on machines except to do the initial screening; people do it. We insist on human judgment. With exceptions already described, NSA is forbidden to collect not only messages to or from U.S. persons, but also information *about* U.S. persons. Fidelity to this rule requires an evaluation of context, and no technology can do this reliably, though it can greatly narrow the universe of relevant data. Some argue that technology and a series of "machine understandable rules" will solve this problem yet. They may be right. The key advances, if and when they come, will be in the areas of mathematical theory, particularly cluster analysis, and language recognition. But those fields, particularly cluster theory, are in a relatively immature state.[25] In any case, most activities do not involve an either/or choice of person or machine. Rather, most systems involve a person directing a machine to do something (*e.g.*, collect all phone calls to or from a phone number, or sell 1,000 shares of XYZ Co.) or reacting to

[24] *Joint Congressional Inquiry,* p. 74.

[25] As to cluster theory, see E.J. Moniz and J.D. Baldwschwielder, "Approaches to Combat Terrorism: Opportunities for Basic Research: Report of a Joint Workshop…," submitted to the National Science Foundation, August 2003, pp. 38–39.

something the machine has done (*e.g.*, analyzing intercepts or re-balancing a portfolio after a sale). Keeping track of these interactions leads us to the question of audit trails.

Principle No. 6: *When technically feasible, audit trails should be created automatically for every significant function of the system—including database queries. The protocol for reviewing audit trails should be written, and where sampling must be resorted to, the rationale for the sample should be made part of the record.*

Regrettably, making an audit trail is only the beginning and not the end of the task, because someone has to examine that audit trail. Depending on the system involved, one person may be able to review every item in the audit trail every day; or the trail may be so voluminous that it can only be sampled at longer intervals. In fact, most auditing today is based on sampling. If the audit is to have probative value, however, the reasoning behind the size, timing, and focus of the sample is critical. In my experience, financial auditors are better at this aspect of the business than program auditors; they have more experience with it and give more thought to it, partly because the liability consequences of failure force them to do so. Governmental organizations with program oversight responsibilities, including my own, need to do better in this area.[26]

No one makes a record of everything, by the way. It would be unusual, say, to try to create an audit trail of the occasions on which any two managers talk in the elevator. Doing so would be expensive, unreliable, and usually pointless, and it would be a significant burden on doing business. The decision to create an audit trail involves a combination of cost-benefit and risk analysis. At NSA, where toleration for misbehavior is low and risks are often high, we increasingly insist on audit trails.

One great advantage of technology is that it can often drastically narrow the scope of an audit. Some years ago I visited a securities industry client that was particularly proud of its technological prowess. Its reputation and market niche were based on its use of a "black box" to perform basic trading functions that its competitors performed in the old fashioned, face-to-face way. But when I visited its back office operations I encountered a compliance staff busily poring over columns of data—by hand! They were doing detective work: looking for irregular trades, that is, trades that violated one or another of the many rules that govern that business. If a trade would violate a rule, or if tasking a U.S. phone number would be against the law, why search for it later like a needle in a haystack? Accordingly:

Principle No. 7: *To the extent feasible, the operational function of the technology and the audit function should be collapsed. That is, if an operation is forbidden, the machine should be incapable of executing it.*

When this can be done, you eliminate the need for after-the-fact detective work and instead impose a preventive control. Life is usually not so simple, however, because inevitably there are exceptions. Is it unlawful for NSA to task a U.S. phone number? Yes, but not if it's a phone number covered by a FISA warrant, for example. There is no single correct way to handle exceptions. Rules may vary among systems; the need for urgent handling will vary according to circumstance; the size of the problem may make particular solutions impractical; and so forth. As a general matter, however, I would say:

Principle No. 8: *Where an operation is only conditionally forbidden, exceptions should be documented and auditable with clear lines of accountability, and exception reports should be generated automatically. Written approval to override a conditional rule should be required at a supervisory level—before the fact, if practicable.*

The information handled by intelligence agencies is generally handled on a "need to know" basis. Sensitivity naturally led to careful ways of doing business. If you didn't need to write something down, you didn't. If you had to write it down, you showed it to whoever needed to see it

[26] For a concise discussion of financial audit controls and their applicability to federal agencies, see KPMG LLP, "Federal Agencies—Will Sarbanes-Oxley fit? A Discussion of Federal Internal Controls," 2004.

and then put it in a safe. As to your agent on the far side of the world, he was on his own. If you communicated with him at all, it was sporadically, usually by typing a message in all caps over a secure cable.

That was another world. Today, just as in the private sector, a large part of the intelligence business is carried on via e-mail and other electronic links. When you write something down, it more often goes into a database than a safe. This makes information sharing possible on a wide scale. But information sharing is inimical to information security. If only one person knows something, and if the risk of compromising that information through intentional leaking, carelessness, theft, etc. is assumed to be x, then disclosing the information to a second person at least doubles the risk. When the information is put in an electronic database, even if it is intended to be shared by only one other person, the risk of disclosure increases exponentially. Information sharing and information security are therefore in constant tension and involve the daily balancing of risk. Detailing procedures for that balancing would be beyond the scope of this article, but I will state a basic proposition:

Principle No. 9: *Access to databases should be restricted by policy and technology to those persons who need it.*

This deceptively simple principle is actually difficult to implement. Apart from the risk-fraught decision of granting access, a major administrative challenge is keeping accesses current. Unless accesses are rigorously reviewed at frequent, established internals, the need-to-know principle will go to ruin in no time. Which brings us to an important corollary: *The software in the organization's human resources department should be engineered to fit seamlessly with the software that governs electronic access, so that when a person changed jobs in the organization, access would be immediately and automatically shut off unless again justified.*

Another challenge is the segmentation of databases. We build increasingly powerful databases with large numbers of data fields that are populated by data gathered from different sources for different purposes. When potential new users of the data request access to it, however, they typically seek access to an entire database rather than to the data required to address a particular need. Sometimes a narrower access can be tailored. If not, refusing access may be contrary to the imperative to share information with those who need it, but granting access may mean that the requestor gets sensitive information for which he or she has no need—unless the database is segmented. Figuring out how to share information more widely requires re-thinking who needs to know; it does not require abandoning the need-to-know principle.

Addressing these technical issues requires a lot of money and a high degree of skill. As everyone concerned with oversight knows, however, oversight is in constant competition with the operational mission for resources, no less in the public than in the private sector. This is normal. As a practical matter, however, it is difficult to persuade managers to expend resources to modify existing systems that may work quite well from an operational viewpoint. *It is therefore vital that Principles 6 through 10 be reflected in new systems before they come on line. For that to happen, money must be requested by the intelligence agencies for these purposes and for related research, and then authorized and appropriated specifically for these purposes by Congress.* Ensuring that this happens is exactly the kind of structural and policy-level oversight for which the Intelligence Committees are well suited.

Principle No. 10: *No system of oversight will be effective unless it includes a methodical program of monitoring to see that corrective actions are implemented.*

The effectiveness of NSA's IG Office was enhanced enormously when it put in place a dedicated, computerized system to follow up all recommendations adopted by the Director and to monitor their implementation. At NSA, this function "is extremely effective and is an example of a best practice that other Offices of Inspectors General in the intelligence community should be encouraged to use."[27] Without such a system, changing the way a bureaucracy works is a hit-or-miss proposition. It is also important to staff this function with experienced people who stay in the job long enough to make a contribution to the institutional memory. Frequently rotating people through this job is not smart. It is surprising how many oversight operations do not include a rigorous follow-up function.

Policy Lessons

NSA and its sister intelligence agencies did not suddenly wake up in 1976 and decide that oversight and compliance were good business. They were made to reform themselves under overwhelming pressure, and the process was painful. The Agency's current leadership, however, clearly understands the relationship between oversight and trust and has endorsed rather than tolerated a robust and energetic Office of Inspector General as a tool for improving efficiency as well as for ferreting out misbehavior. Director Hayden has noted that every society must decide for itself where to plant its flag on the continuum between security and liberty; and in this country, where we have always planted it closer to liberty, that decision will continue to be made by the elected representatives of the American people, acting under the Constitution of the United States.[28] This is an astonishing statement from the head of an organization born in secrecy and learned in the black arts of signals intelligence, and it represents a profound institutional evolution.

This brief history, and the oversight principles that come from it, hold lessons for those who think about information and national security. First, for our existing intelligence agencies, the trick will be to keep them on the law's leash without drawing their claws. Failure to encourage robust and imaginative intelligence will place the nation in continual jeopardy of further attack, and failure to do so in accordance with the law will produce the kind of backlash against the agencies that came after 1976. Either kind of failure will be judged harshly. Second, for those agencies now on the drawing boards, foreign or domestic, the challenge will be to build cultures and systems of compliance that implement the lessons of the last quarter century—not after a compliance breakdown for which the public will have little tolerance, but right from the start. The budgetary and policy implications of these goals should not escape the intelligence community or its congressional overseers.

—Joel F. Brenner is Inspector General, National Security Agency/Central Security Service.

[27] Office of the Inspector General, Department of Defense, "Management Review of the Office of the Inspector General, National Security Agency," May 23, 2003, pp. 5–6.

[28] Lt. Gen. Michael V. Hayden, USAF, Speech Before the American Bar Association, Standing Committee on Law and National Security, Washington, D.C., April 18, 2002.