2008

National Security Letters and Intelligence Oversight

Michael J. Greenlee
Concordia University School of Law, mgreenlee@cu-portland.edu

Follow this and additional works at: http://commons.cu-portland.edu/lawfaculty
Part of the First Amendment Commons, and the National Security Law Commons

CU Commons Citation

This Book Chapter is brought to you for free and open access by the School of Law at CU Commons. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of CU Commons. For more information, please contact libraryadmin@cu-portland.edu.
National security letters and intelligence oversight

Michael J. Greenlee

Introduction

For nearly 30 years, national security letters (NSLs) have served intelligence agencies as a powerful tool for collecting information. Although the initial NSL statute created a weak and often ineffective means of requesting information from financial institutions, NSL powers and authorities have developed over the years to become a vital component in the conduct of successful counterintelligence and terrorism investigations – described by some FBI personnel as “our bread and butter.” The information gathered through NSL requests often provides essential evidence that is required to obtain more invasive tools for intelligence gathering such as wiretaps, pen register/trap and trace devices, and search warrants. Given the potential for abuse in using these tools to gather highly personal information, Congress has sought to balance the investigative needs of intelligence agencies with the legitimate privacy and civil liberty interests of the individuals against whom these powers are used.

National security letters are a type of administrative subpoena principally used by the Federal Bureau of Investigation (FBI) in foreign intelligence, counterintelligence and terrorism investigations. Although originally used to collect customer transactional records from financial institutions, NSL powers and authorities were later expanded to include transactional records from electronic communication providers and consumer credit agencies. Transactional information provides evidence of financial or communication transactions without necessarily revealing the substance of those transactions. For example, telephone and e-mail transactional information could include historical information on telephone calls made and received from a specified number; billing records; subscriber information including name, address, and length of service; and e-mail addresses associated with an account. What is not included in transactional information is the content of these communications.

An important and controversial aspect of NSL powers is the ability of the issuing agency to enforce a nondisclosure provision, or “gag order,” against NSL recipients. A gag order prevents recipients from disclosing to anyone that they have received a national security letter request or from revealing any details connected to the investigation. The original nondisclosure provisions served
The deployment of the mosaic theory to justify such deference can be seen as yet another example of the Bush administration's advocacy of the "unitary executive" and its desire to insulate executive actions from congressional and judicial review. Such a move by the executive branch would unravel hard-won privacy and civil liberty protections that have proven so necessary in the conduct
of intelligence investigations and leave those persons against whom NSL powers are used with no effective recourse when those powers are abused. The Church Committee concluded that if Americans confronted their mistakes and resolved not to repeat them, they would remain a people worthy of the best of their past. In the case of national security letter powers and authorities, and what amounts to an unchecked restriction of free speech, it would appear that the current administration is rushing to prove itself unworthy of such distinction.

National security letters prior to the USA PATRIOT Act

The structure of the contemporary U.S. intelligence community would not have been possible if it were not for the investigations conducted by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence – also known as the Church Committee. For 17 months in 1975 and 1976, the Church Committee’s comprehensive investigation of the intelligence community revealed a horror show of government abuse in which intelligence agencies had acted virtually without oversight or restraint and with utter disregard for the law over a 30-year period. Among the many documented instances of abuse, the Church Committee revealed numerous cases where intelligence agencies had conducted investigations of U.S. citizens who were not engaged in, or even suspected of, any criminal activity. Information gathered during these investigations was quite often illegally obtained and broadly disseminated between intelligence and law enforcement agencies. In some cases, this information was used to disrupt, discredit, or destroy the lives and reputations of certain individuals deemed to be subversive or national security risks – most notably, the intensive effort of the FBI to neutralize and discredit Dr. Martin Luther King, Jr., as an effective civil rights leader.

Despite the broad opposition to the Committee’s investigation from the government, the media and the public, the Committee’s findings and recommendations led to the implementation of a series of safeguards to restrict the collection and sharing of information about Americans by the FBI and other intelligence agencies. The most significant result of these investigations was the passage of the Foreign Intelligence Surveillance Act of 1978 (FISA) and the creation of the Foreign Intelligence Surveillance Court (FISC) to provide congressional and judicial oversight of foreign intelligence investigations. This Act, in addition to subsequent Attorney General Guidelines and presidential executive orders, led to a complete reformation of the conduct of intelligence investigations within the United States and served as a stable framework preventing the recurrence of past abuses. It was within this framework that national security letters were developed as one of the FBI’s vital intelligence-gathering instruments.

The first mention of the administrative tools that would later be known as national security letters is in the Right to Financial Privacy Act of 1978 (RFPA). Two years earlier, the Supreme Court had held in United States v. Miller that bank customers had no legitimate expectation of privacy concerning
transactional information kept in bank records, and therefore, subpoenas issued by government authorities for such information created no intrusion upon customer Fourth Amendment rights.\textsuperscript{19} Recognizing the highly personal nature of the information that such records might contain, Congress responded to \textit{Miller} by passing the RFPA, which provided protection of individual rights beyond that afforded in the Constitution.\textsuperscript{20} Nevertheless, Congress recognized the importance of creating a proper balance between the right to privacy and the need of law enforcement agencies to obtain financial records in their investigations.\textsuperscript{21}

Section 1114 of the RFPA established the provisions for the release of financial information in foreign intelligence investigations.\textsuperscript{22} Included in this forerunner to the modern NSL is a nondisclosure provision prohibiting the financial institution from disclosing to any person that a government authority has sought or obtained access to a customer’s financial records.\textsuperscript{23} In particular, Section 1114 did not mandate compliance by the financial institution\textsuperscript{24} but only required certification that the NSL request complied with statutory requirements.\textsuperscript{25} Section 1114 also made no mention that the gag order could be challenged, lifted, or judicially enforced. The need for nondisclosure is briefly addressed in the House reports accompanying the original RFPA and in the 1986 amendments to the RFPA. Although the final version of the 1978 Act represented a “substantial compromise between the original version of the title and the views of various law enforcement agencies,”\textsuperscript{26} there is nothing to suggest that the imposition of a nondisclosure provision in foreign intelligence investigations was part of this discussion. There is brief mention of the nondisclosure provision, stating that nondisclosure is needed in order to assure the absolute secrecy required in foreign intelligence investigations.\textsuperscript{27} Likewise, the House report accompanying Public Law 99-569,\textsuperscript{28} amending the RFPA, notes that the effective conduct of FBI counterintelligence activities requires such nondisclosure.\textsuperscript{29}

In addition to amending the RFPA in 1986, Congress passed the Electronic Communications Privacy Act (ECPA). This Act granted the FBI access to telephone company subscriber information, toll billing records and other electronic communication transactional records, comparable to the access to transactional records the FBI was provided under the RFPA.\textsuperscript{30} The nondisclosure provisions contained in ECPA and in the amended RFPA are nearly identical.\textsuperscript{31}

The 1986 amendments made significant changes to the standard for issuing an NSL. Where the original RFPA required only certification from the appropriate authority and did not mandate compliance, the amended RFPA and ECPA statutes required certification that the information was “relevant to”\textsuperscript{32} or “sought for”\textsuperscript{33} foreign counterintelligence purposes. In addition, NSL requests were required to show specific and articulable facts giving reason to believe that the target of the investigation is a foreign power or the agent of a foreign power. The “specific and articulable facts” standard was created specifically for use in counterintelligence investigations, balancing consumer privacy interests with the needs of law enforcement officials to maintain secrecy in their investigations.\textsuperscript{34} Both statutes also made NSL compliance mandatory.\textsuperscript{35} However, neither statute
addressed the lack of specific language permitting a recipient to request judicial review to challenge, lift or modify an NSL or its nondisclosure provision.

In 1996, Congress created the final FBI national security letter authority when it passed amendments to the Fair Credit Reporting Act (FCRA). These amendments authorized FBI access to consumer credit agency reports during counterintelligence investigations. Like the previous NSL statutes, Section 601 of the FCRA Amendments was “carefully crafted” to protect consumers’ rights to privacy while allowing law enforcement agencies to obtain necessary information in foreign counterintelligence investigations. The expansion of NSL authority was “not taken lightly,” and the House and Senate conferees concluded that the need was genuine, that the threshold for use sufficiently rigorous, and that the built-in safeguards minimized the threat to privacy. To effectively use the powers it had been granted under the Right to Financial Privacy Act, the FBI considered access to credit agency records a crucial requirement to trace the financial activities of suspected spies or terrorists.

The nondisclosure provision created in Section 624(d) departed from the parallel provisions found in ECPA and the RFPA by clarifying that disclosure was permitted within the contacted institution to the extent necessary to fulfill the request. Interestingly, the Conference Report states that although the conferees did not take a position on whether similar disclosures would be forbidden under the RFPA (which, like the ECPA, lacked such clarification), it notes that practicalities would dictate that the provision not be interpreted to exclude such disclosure. In another departure from the ECPA and RFPA provisions, the FCRA amendments authorize judicial enforcement of NSLs. Once again, no provision was made for recipients to challenge or modify an NSL in court.

In creating these NSL authorities, Congress sought to balance legitimate privacy interests with the investigative needs of law enforcement, especially in cases of foreign counterintelligence investigations. What began as a rather ineffective tool for gathering intelligence information developed into an effective and vital instrument providing carefully crafted safeguards to minimize the threat to privacy. All of the authorization acts produced informative legislative histories, which include extensive discussion of the privacy issues that were of concern at the time. However, the constitutionality of NSL gag orders was apparently not among those concerns. Congress recognized that nondisclosure was necessary for the successful conduct of foreign counterintelligence investigations. The fact that no mechanism existed, whether administrative or judicial, for modifying or terminating a nondisclosure order apparently failed to inspire any significant debate concerning the effect of permanently restricting speech.

If Congress was remiss in not providing procedural protections concerning NSL powers, it was apparently of little concern to those individuals and groups against whom nondisclosure was being enforced. Prior to passage of the USA PATRIOT Act, no court challenges to NSL gag orders were filed under any of the then existing statutes; it was not until 2004 that a judicial challenge to NSL powers and authorities was raised.
Changes to NSL powers and authorities in the USA PATRIOT Act

The USA PATRIOT Act was signed into law on October 26, 2001, less than seven weeks after the al Qaeda terrorist attacks in the United States. Despite the sweeping changes it made to the investigative tools and procedures used by law enforcement agencies to investigate and prosecute terrorism, the USA PATRIOT Act encountered little opposition in either the House or Senate. However, the broad expansion of intelligence and law enforcement powers under the USA PATRIOT Act generated considerable concern over the prospect of government abuse.

Congress recognized the possibility of overzealous government agencies infringing civil liberties in their use of these new powers, especially in a time of national emergency. Not surprisingly, the domestic surveillance and intelligence abuses exposed by the Church Committee formed part of the Congressional debate surrounding the PATRIOT Act. Senator Patrick Leahy (Democrat from Vermont) urged the Senate to recall the Cold War abuses of investigative powers by federal agencies that had acted under the rubric of protecting national security. During a time in which the executive branch had a free hand in using the FBI and the Central Intelligence Agency (CIA) to conduct domestic surveillance, with no oversight by Congress or the courts, massive files were compiled on U.S. citizens based solely on activities protected by the First Amendment. Senator Leahy and others were especially concerned that provisions of the USA PATRIOT Act – which made sweeping changes in the relationship between law enforcement and intelligence agencies, allowed the sharing of information broadly defined as “foreign intelligence,” and lowered the standards for acquiring such intelligence – could serve as an invitation for government abuse and disrupt the protective framework of intelligence oversight that had emerged as a result of the Church Committee’s findings.

In the end, Congress initiated a series of safeguards to ensure against unnecessary and improper use of the powers granted under the new law. Most importantly, Congress created a sunset provision that would require 16 sections of the USA PATRIOT Act to expire on December 31, 2005, unless specifically renewed by Congress. These sections included some of the most troublesome provisions of the USA PATRIOT Act concerning wiretapping, the sharing of intelligence information with law enforcement agencies, and access to business records. Nonetheless, many groups continued to fear that the expansion of surveillance powers under the USA PATRIOT Act would significantly weaken important civil liberty protections.

Section 505 of the USA PATRIOT Act (“Miscellaneous national security authorities”) broadened the FBI’s NSL authority by amending three of the four existing NSL statutes and adding a fifth. These changes included eliminating the relevance standard and the need to show specific and articulable facts; expanding the scope of investigations beyond foreign counterintelligence to also include international terrorism or espionage; allowing Special Agents in Charge
of FBI field offices to approve NSLs; and adding a caveat that no investigations of American citizens can be based exclusively on First Amendment-protected activities. A fifth NSL authority was created by amending the FCRA to permit the FBI and other federal agencies to use NSLs to obtain consumer full credit reports. Although Section 505 reduced the standard for obtaining an NSL and expanded the scope of NSL power and authority, it was not included among those provisions designated to sunset in 2005.

The many changes made by the USA PATRIOT Act to law enforcement and intelligence investigations did not extend to NSL provisions concerning nondisclosure. Also, the deficiencies of preexisting NSL authorities – such as a lack of judicial enforcement mechanisms, the absence of penalties for noncompliance, and the lack of explicit provision allowing recipients to challenge NSL requests – remained. Nonetheless, changes (or the lack of changes) to NSL powers continued to fly under the radar. It was not until the 108th Congress that amendments were first proposed to remedy some of these deficiencies. These changes would later evolve into the NSL amendments found in the USA PATRIOT Improvement and Reauthorization Act of 2005.

Challenges to NSLs: Doe v. Ashcroft and Doe v. Gonzales

The first constitutional challenges to national security letters were raised during the 109th Congress. The plaintiffs in Doe v. Ashcroft (hereinafter Doe I) and Doe v. Gonzales (hereinafter Library Connection) argued that NSL statutes could not withstand constitutional scrutiny unless more explicit provisions were made for judicial review and permissible disclosure by NSL recipients. Both involved only NSLs issued under 18 U.S.C. § 2709 concerning electronic communications.

Doe I raised both Fourth Amendment and First Amendment challenges. In that case, an unnamed internet service provider (ISP) received an NSL requiring the production of consumer records pursuant to § 2709. The ISP challenged the NSL, claiming that (1) the lack of an explicit judicial review mechanism under § 2709 resulted in the compulsory secret and unreviewable production of information, in violation of the Fourth Amendment; and (2) the sweeping permanent gag orders lacking any type of judicial review mechanism violated free speech protections under the First Amendment. The district court agreed with the ISP on both challenges, finding that in all but exceptional cases, § 2709 had the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the Fourth Amendment, and that universally applied gag orders imposing perpetual secrecy and demanding unremitting concealment placed a disproportionate burden on free speech under the First Amendment.

In reviewing § 2709(c), the court found that since the nondisclosure provision operated as a content-based prior restraint on speech, it should be subject to strict scrutiny review. Under strict scrutiny, a speech restriction that is either content based or acts as a prior restraint is presumptively invalid and may be upheld only if the government can demonstrate that the restriction is narrowly
National security letters 191
tailored to promote a compelling government interest. If a less restrictive alternative would be at least as effective in achieving the legitimate purpose that the statute was created to serve, then the speech restriction cannot be defined as narrowly tailored.

The district court stated that nondisclosure provisions acted as a prior restraint based on “the straightforward observation that it prohibits speech before the speech occurs.” The court rejected the government’s argument that § 2709(c) did not act as a prior restraint because the statute did not create a licensing scheme by which the government could pick and choose among speakers to restrain. Instead, the court found that a blanket permanent prohibition on future disclosures was an even purer form of prior restraint than a licensing system, comparable to the most severe form of a licensing system in which no licenses are granted and the speech at issue is maximally suppressed.

The court also found that the nondisclosure provision acted as a content-based restriction. The government had argued that since nondisclosure provisions acted in a content-neutral manner, they could not be considered content based. The government explained that it was not seeking to silence “less favored” or “controversial views”; rather, the prohibition on speech applied irrespective of any particular speaker’s views. However, the court found that even a viewpoint-neutral restriction can be content based if the restriction pertains to an entire category of speech. In the case of § 2709(c), recipients were forever barred from speaking to anyone about their knowledge and role in the events pertaining to an NSL, even at a time when disclosure of the investigation might have ceased to generate legitimate national security concerns.

On the basis of these findings, the court applied strict scrutiny in reviewing whether nondisclosure orders were narrowly tailored to promote a compelling government interest. Although accepting the government’s argument that the conduct of international terrorism and counterintelligence investigations could demonstrate a compelling government interest to protect national security and that it may be necessary to impose secrecy for long periods of time, the court rejected the government’s argument that a permanent application of nondisclosure orders to all persons affected, in every case, was narrowly tailored.

Looking to then-pending legislation in Congress, the court found examples of less restrictive alternatives that could equally serve the government’s compelling interest without imposing a categorical, perpetual ban on speech. The government countered that such alternatives would be less effective because they would require the government to weigh the risk of court-ordered disclosure against the need for the information sought each time it considered issuing an NSL. The court characterized the government’s argument as tangential to the issue at hand – like “using the edge of the hammer to hit the nail.” The issue of indefinite secrecy imposed by § 2709(c) had little or nothing to do with the government’s ability to gather information; rather, the question was the government’s need to maintain the secrecy of discrete information and to restrict speech long after the investigation had served its purpose. The court granted that a blanket rule swearing everyone to secrecy forever certainly would be the
easiest and most efficient course for the government; however, such a course would not necessarily be the most equitable and protective of fundamental rights. The court concluded that the government failed to carry its burden to show that the extraordinary scope of § 2709(c) was narrowly tailored to achieve its goals.

The court also briefly addressed the government’s deployment of the mosaic theory in arguing for judicial deference to executive-branch national security expertise. The government argued that the court should defer to executive expertise in the case of NSL nondisclosure provisions when the government asserts that such secrecy is necessary for national security purposes. Although the court acknowledged that the judiciary should defer to executive expertise in national security matters, such deference should be conditioned on the specific facts and rationales concerning a particular situation involving particular persons at a particular time (emphasis in the original). Furthermore, the government had cited no authority to support the open-ended proposition that it may universally apply general principles to impose perpetual secrecy on an entire category of future cases for all times and places. Essentially, the government was asking the court to assume that its use of § 2709 would always sufficiently advance asserted government interests to justify the abridgment of First Amendment expressive activity. Unwilling to accept such a dubious assumption, the court found § 2709(c) to be facially unconstitutional. In addition, the court found that since § 2709(c) could not be severed from the remainder of the statute, § 2709 in its entirety should be struck down. Since all NSL nondisclosure provisions operate under the same mechanisms as found in ECPA, it seems reasonable to assume that RFPA and FCRA nondisclosure provisions would also be rendered unconstitutional.

Library Connection followed much the same reasoning as Doe I concerning NSL nondisclosure provisions. In Library Connection, a library consortium – Library Connection – offering internet access to its patrons received a § 2709 NSL requesting the subscriber and billing information for a 45-minute time period relating to a potential terrorist threat. Library Connection filed First and Fourth Amendment challenges similar to Doe I. However, the court only addressed the First Amendment challenge to the constitutionality of the § 2709(c) nondisclosure provision, which prevented Library Connection from revealing its identity as an NSL recipient. The district court reached the same conclusion as Doe I on the nondisclosure issue. After finding that § 2709 constituted a content-based prior restraint on speech, the court applied strict scrutiny to determine whether the statute was narrowly tailored to achieve the government’s compelling interest. Although the court accepted the government’s claim that preventing an NSL recipient from disclosing its identity could serve a compelling interest, it found nothing in the record to support that conclusion as applied in this case. Instead, the court found the government’s argument that disclosure of Library Connection’s identity “may” or “could” harm investigations related to national security too speculative to show a compelling interest. In addition, even if the government’s interest
were more broadly defined as preventing an unknown subject of the government’s investigation from learning of the existence of that investigation, the court found that the restraints and restrictions of § 2709(c) which served that interest lacked the narrow tailoring necessary to survive constitutional strict scrutiny. The court concluded that the government failed to show a compelling interest that would be served by gagging the plaintiffs, and granted Library Connection’s motion to enjoin enforcement of the nondisclosure provision.

In both Doe I and Library Connection, the district courts issued a stay of enforcement pending an appeal before the Second Circuit. While the case was under consideration, the identity of the plaintiff, Library Connection, was revealed through a story in the New York Times, which led to a curious standoff between the government and the plaintiffs. Through an oversight by the government, the name “Library Connection” had not been redacted from part of the records that were publicly available through a court-operated website. Despite the widespread publication of this information, the government insisted that the nondisclosure order be enforced, preventing Library Connection from confirming its identity as an NSL recipient. This led to a bizarre situation in which the identities of the Library Connection plaintiffs were publicly exposed, but the individual plaintiffs could not confirm to anyone, including family members, that they were involved in a national security investigation. It was only after passage of the USA PATRIOT Improvement and Reauthorization Act in March 2006 that the government ceased enforcement of the nondisclosure order against Library Connection. Finally, in June 2006, the government officially withdrew its NSL request from Library Connection, stating that it had used other means to obtain the information. By November 2006, the government was no longer seeking to obtain information from the ISP in Doe I, but nonetheless still sought enforcement of the nondisclosure order.

The USA PATRIOT Improvement and Reauthorization Act of 2005

While Doe I and Library Connection were on appeal, a larger congressional debate was taking place concerning the reauthorization of the USA PATRIOT Act. Sixteen sections of the USA PATRIOT Act were set to expire on December 31, 2005. Most of these provisions concerned surveillance and information sharing in intelligence investigations. In the debate leading up to the expiration of a raft of PATRIOT Act provisions, the federal government, civil liberty organizations and other groups argued both for and against the continuing need for the relevant measures. Some parties favored making the sunset provisions permanent or extending the sunset date, citing the dangers to national security that would emerge if law enforcement and intelligence agencies were stripped of crucial powers needed in the War on Terror; other groups favored either allowing the provisions to expire as planned or allowing their continued use only after serious revisions had been made to better protect civil liberties. Although Section 505 of the USA PATRIOT Act was not included among the sunset
provisions, national security letters formed a significant part of the discussion about infringements on civil liberties.\textsuperscript{74}

The procedural protections that national security letters had lacked since their inception became a focus of the civil liberty debate. Several bills were introduced calling for explicit mechanisms for judicial review and enforcement of NSL requests, clarification of the scope of nondisclosure orders, judicial review of nondisclosure orders, more congressional oversight, and the removal of libraries and booksellers from NSL requests.\textsuperscript{75} The intense public debate surrounding NSLS was felt in Congress, which once again sought to carefully balance the investigative needs of law enforcement and intelligence agencies with legitimate privacy interests.

After months of political wrangling, including a temporary extension of the sunset provision, Congress passed the USA PATRIOT reauthorization statutes - Public Laws 109-177 (PIRA) and 109-178 (ARAA).\textsuperscript{76} PIRA incorporated many of the procedural protections that had been lacking in NSLS. For the first time, provisions were created for judicial enforcement and judicial review of NSL requests;\textsuperscript{77} specific penalties were defined for noncompliance with NSL requirements;\textsuperscript{78} clarifications were added permitting NSL recipients to contact their attorney or anyone else necessary for them to comply with NSL requests;\textsuperscript{79} congressional oversight was expanded;\textsuperscript{80} and a procedure was created for lifting the nondisclosure requirement.\textsuperscript{81} These changes applied to all NSLS issued under the RFPA, ECPA, and FCRA. In addition, libraries not acting as an electronic communication service provider were excluded from NSLS issued under 18 U.S.C. § 2709.\textsuperscript{82}

Sections 115 and 116 of PIRA established the procedure for imposing a nondisclosure order and providing judicial review to challenge enforcement of nondisclosure. To impose a nondisclosure order on an NSL recipient, the Director of the FBI or his designee must certify that nondisclosure is required to protect national security, to prevent interference with an ongoing investigation or with diplomatic relations, or to protect the life or physical safety of any person.\textsuperscript{83} After receiving an NSL, recipients can challenge the request and the nondisclosure order in a federal district court.\textsuperscript{84} The district court may modify or set aside the nondisclosure order if it finds no reason to believe that the original certification requires continued enforcement.\textsuperscript{85} However, if a designated official\textsuperscript{86} certifies that disclosure might endanger national security or interfere with diplomatic relations, then such certification is conclusive and the nondisclosure order remains in force.\textsuperscript{87} NSL recipients are allowed to challenge nondisclosure orders once per year.\textsuperscript{88} If a nondisclosure order is challenged one year or more after the original NSL request, then the order must either be terminated within 90 days or a designated official must recertify the need for nondisclosure.\textsuperscript{89} Once again, it is conclusive for a designated official to certify that nondisclosure is necessary.

In amending the NSL statutes, Congress apparently had given heed to the civil liberty concerns expressed by the public, the courts and its own members by providing much-needed procedural protections, clarifications and additional
oversight. These changes had an immediate effect on *Doe I* and *Library Connection*, which were on appeal before the Second Circuit when PIRA was passed. The PIRA amendments provided the explicit pre-enforcement judicial review that the respective district courts had found lacking in the original NSL provisions. In light of the congressional actions taken in 2005, which empowered NSL recipients to challenge the issuance of an NSL in court and freely communicate about an NSL request with their attorneys, the ISP in *Doe I* dropped its Fourth Amendment claims. Likewise, the Fourth Amendment portion of the district court opinion was vacated. The ISP’s original First Amendment claims in *Doe I* were also vacated, and the case was remanded to the district court to address the constitutionality of the revised § 2709(c) and the new standards for judicial review of nondisclosure orders. As was mentioned earlier, the issues in *Library Connection* became moot when the government dropped its opposition to the plaintiff’s disclosure of its identity and withdrew its demand for the requested information.

### The mosaic theory, judicial deference and NSL nondisclosure

Despite the procedural protections provided by PIRA, some groups believed the amendments did not go far enough to protect civil liberties. The American Civil Liberties Union (ACLU), for example, accused the Bush administration of “stacking the deck” in the government’s favor:

> Under the new law, if a high-level political appointee certifies that national security or diplomatic relations will be harmed, the court must consider that assertion “conclusive” unless the recipient proves that assertion was made in “bad faith” – meaning the gag order will stand. This plainly unconstitutional standard fails to comport with Americans’ First Amendment rights.

This statement formed the basis of the ISP’s argument in the remanded case before the district court. The ISP argued that the amended nondisclosure provisions violate the First Amendment and the principle of separation of powers because they prevent courts from applying a constitutional standard of review, fail to provide constitutionally mandated procedural safeguards, and invest the FBI with unbridled discretion to prohibit speech. In passing PIRA, the ISP claimed Congress overstepped the bounds of separation of powers by dictating to the courts how they must adjudicate First Amendment claims when considering nondisclosure challenges and by requiring the courts to apply a standard of review that contemplates “near-servile deference” to the executive. The underlying rationale used by the government to justify such judicial deference is found in the mosaic theory.

Mosaic theory claims are commonly used by federal agencies seeking to deny disclosure of information requested under the FOIA. The FOIA generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are
protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. Exemption I of the FOIA allows agencies to prevent disclosure of all national security information concerning intelligence collection, the national defense or foreign policy that has been properly classified. In conjunction with Exemption 1, Exclusion (c)(3) allows the FBI to deny the existence or nonexistence of certain records pertaining to counterintelligence, foreign intelligence or international terrorism. Through the use of NSL gag orders, the executive also has the ability to prevent the disclosure of information that may threaten national security or interfere with intelligence investigations, similar to the exemptions allowed under FOIA. However, where the FOIA allows the federal government to deny access to information in the possession of the government, nondisclosure prevents NSL recipients from revealing information they already know.

In support of its decision to withhold information under the FOIA or to prevent disclosure in the case of NSLs, a federal agency will sometimes advance a mosaic claim. Such claims usually state that access to the requested materials must be denied because, when combined with other discrete bits of information, the resulting mosaic of information could reveal vital facts concerning national security. Ordinarily, judges do not have the national security expertise that would enable them to understand the sensitivity of an isolated piece of information in the context of the intelligence apparatus. Congress, the executive, and the courts all agree that the mosaic theory is basically correct: executive-branch intelligence agencies are the experts in matters relating to national security, and their judgments concerning these issues should be deferred to by the other branches of government. The real point of contention concerns the level of deference that the executive should be granted in these matters. Disagreement concerning proper deference occurs not only among the three branches of government, but within the judiciary itself. This variance of opinion within the judiciary has led to the emergence of three levels of deference.

Some courts have shown nearly complete deference, amounting almost to an abdication of judicial review. Other courts are reluctant to evaluate and challenge mosaic claims, preferring to treat them as a distinct and privileged defense of secrecy. These courts show an augmented form of deference that amounts to an effective delegation of mosaic theory oversight to the agencies themselves. A third set of courts have opposed the application of any special treatment and evaluate mosaic claims with the standard deference due to the government in national security litigation. Most courts have been willing to either delegate or abdicate to executive expertise in matters of national security, resulting in the phenomenal success of mosaic claims in the context of denying FOIA requests. However, courts choosing to apply standard deference when reviewing mosaic arguments have generally rejected such claims.

Between 1972 and 2001, only one court rejected outright an agency’s mosaic argument involving an FOIA request. Since 2001, one other court has rejected an agency mosaic argument implicating the FOIA. In addition, three courts have rejected mosaic claims when considering the constitutionality of government...
actions restricting First Amendment rights. As was discussed earlier, *Doe I* and *Library Connection* rejected mosaic claims supporting the unconstitutional application and enforcement of nondisclosure orders. The Sixth Circuit in *Detroit Free Press* also found unconstitutional a mosaic intelligence argument concerning the closure of certain immigration removal proceedings under the “Creppy Directive.”108

The courts in *Doe I*, *Library Connection* and *Detroit Free Press* applied standard deference in reviewing the government’s mosaic claims. These courts rejected the government’s mosaic theory argument for basically the same reason: In each case, the government failed to show that the restriction in question was narrowly tailored to promote a compelling government interest. *Doe I* and *Library Connection* found universally applied gag orders imposing perpetual secrecy on disclosures that “may” or “could” harm national security investigations to be too speculative and not narrowly tailored. Similarly, *Detroit Free Press* found that categorically and completely closing all special interest hearings without demonstrating, beyond speculation, the absolute necessity of such closure did not meet the requirements of strict scrutiny review.109

In exposing the unconstitutional manner by which the government was attempting to restrain First Amendment-protected rights, it would seem that the vital necessity for courts to engage in standard deference review of national security mosaic claims would be clear. Nevertheless, the PIRA amendments appear to leave the judiciary no choice in matters concerning nondisclosure orders. Certification by designated officials is considered “conclusive” in nondisclosure challenges when national security or diplomatic relations are threatened. Since such language seems to allow little room for courts to apply standard deference, all that remains, apparently, is for courts to either delegate or abdicate their review power to executive expertise. This has led to accusations that judicial review of nondisclosure orders is merely a rubber stamp, purely cosmetic, stunted, and a fig leaf.110 The government denies this is the case, stating that district courts can request additional information from the government to ensure that the certification is supported by specific facts or rationales tied to the situation at issue.111 However, this interpretation of the court’s ability to review government certification is supported by neither the legislative history of PIRA nor the filings submitted in *Doe I*.

Statements in the conference report and congressional debates accompanying the PIRA amendments indicate the level of deference that was anticipated by members of Congress. The conference report accompanying H.R. 3199 states: “This provision [PIRA Section 115] recognizes that the Executive branch is both constitutionally and practically better suited to make national security and diplomatic relations judgments than the judiciary.”112 This comment is expanded upon in the *Congressional Record*:

The standard in the conference report is the appropriate one, both constitutionally and practically, as it recognizes that sensitive national security and diplomatic relations judgments are particularly within the Executive’s
expertise... It will be an exceedingly rare case in which a judge will find, contrary to a certification by an executive branch official, that there is no reason to believe that the nondisclosure order should remain in place. It will be even rarer for a judge to find that one of the Senate-confirmed officials... has acted in bad faith... I could not have supported the conference report or the explicit judicial review of nondisclosure orders if I thought that they would give judges the power to second-guess the informed... judgments of our high-level executive branch officials. The conference report makes clear that judges will not have such discretion.\textsuperscript{113}

The deference contemplated by the above statements hardly envisions a judiciary that will engage in meaningful review taking into account the "specific facts or rationales" connected to the situation at hand, as asserted by the government. The "rarity" suggested in these remarks by Senator Kyl anticipates the deference exhibited by courts that have either abdicated or delegated their responsibility to review the decisions of the executive when it raises the mosaic theory in its defense. But it is precisely in those cases in which the judiciary has requested specific facts and rationales concerning the particular situation involving particular persons at a particular time that the court has found the mosaic claims asserted by the government to be speculative and lacking justification for the requested restraint of First Amendment rights. However, if courts do not have the discretion to conduct meaningful review, which requires the executive to set forth particular facts for the court to evaluate, then the government will rarely be found to have failed to justify the need for nondisclosure.

For an example of the specificity to be expected from the executive when certifying the need for nondisclosure, the case Doe v. Gonzales is exemplary. The following is the text of the certification submitted by FBI Director, Robert S. Mueller, in its entirety:

I, the Director of the FBI, and an official authorized to certify as to the necessity for the non-disclosure provision, do hereby certify that disclosure that the FBI has sought or obtained access to information or records through the National Security Letter issued on or about February 10, 2004 to the plaintiff John Doe in John Doe v. John Ashcroft, et al., No. 1:04-cv-02614 (U.S.D.C., S.D.N.Y.), including, but not limited to, the disclosure of the NSL itself or its contents, may endanger the national security of the United States.\textsuperscript{114}

According to the text of PIRA Section 115, this certification must be accepted by a reviewing court as \textit{conclusive} since it asserts that disclosure may endanger national security. There is no mention in the certification, the text of PIRA or in the legislative history that a reviewing court has any discretion to request more information from the government to support its need for nondisclosure. In this instance, the mere assertion that national security may be endangered is all the proof that is required of the government.
Conclusion

In March 2007, the Office of the Inspector General (OIG) issued its first review of national security letter use by the FBI. Covering calendar years 2003–04 and 2005–06, the OIG reported the issuance of over 140,000 NSL requests and disclosed significant abuses by the FBI in its use of NSL powers. In the most egregious case of abuse, the OIG reported that the FBI circumvented the requirements of NSL authorities by issuing so-called exigent letters on over 700 occasions. These “exigent letters” stated that the records requested were in connection with fast-paced investigations and that the subpoenas (NSLs) authorizing the request had been submitted for processing and service. However, in most instances there was no documentation associating the requests with pending national security investigations; the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate record keeping; and in many instances, NSLs were only processed and issued many months after the FBI had already obtained the requested information. The OIG also reported that the database used by the FBI to track NSL use was inaccurate and believed the total number of NSL requests issued to be significantly higher than reported.

The current rendition of NSL powers and authorities is unlike anything previously created by Congress and allows the executive to act with little restraint when gathering intelligence. The increased congressional oversight reflected in the OIG Report has shown that more scrutiny of executive intelligence-gathering activities is vital to prevent intentional or accidental violations of privacy and civil liberty interests when NSL powers are invoked. In addition, the decisions of the courts in Doe I, Library Connection and Detroit Free Press demonstrate the importance of applying meaningful judicial review to the certifications of the executive branch to prevent the unconstitutional restraint of First Amendment-protected activities. Although PIRA provides important protections related to NSL use and enforcement, to assume that continued oversight of the executive by the judiciary is unnecessary, or that the acceptance by the judiciary of unsupported assertions concerning continued nondisclosure is unproblematic, is plainly not warranted.

The tension between secrecy, privacy and liberty, which is inherent in intelligence investigations, will always demand meaningful and effective oversight of the executive branch by Congress and the courts. In the case of NSL nondisclosure orders, this will only be achieved if the executive branch is required to present hard facts to the court to support its request for continued nondisclosure. This could be accomplished by amending PIRA and applying the “specific and articulable facts” standard, specifically created by Congress for intelligence investigations in 1986, to recertifications for nondisclosure enforcement. Such a standard would defer to the expertise of the executive branch when initially imposing a nondisclosure order, but would require the presentation of specific and articulable facts if the executive seeks to extend that order after the initial investigation. Such a standard would recognize the limited ability of intelligence
agencies to present such “hard” facts in the initial stages of intelligence investigations, but would require such proof after the executive branch has been given the opportunity to gather intelligence. In this way, balance could be restored by recognizing the needs of intelligence agencies to quickly initiate investigations, but also protect against the prolonged infringement of civil liberties by demanding proof that the investigation has actually “paid off” in terms of intelligence.

The Church Committee revealed in stark detail the extent to which the intelligence community will extend and abuse its powers if left unchecked. “If intelligence agencies continue to operate under a structure in which executive power is not effectively checked and examined, then we will have neither quality intelligence nor a society which is free at home and respected abroad.”

Confronted by an administration that openly advocates for unchecked executive power and authority in the name of protecting national security, such oversight is as necessary today as it was 30 years ago.

Notes


2 There are five federal statutes authorizing the use of national security letters. This chapter will not discuss NSLs issued under § 436 of the National Security Act, 50 U.S.C. § 436 (2000). Section 436 NSLs apply only to executive-branch employees who have consented to a background investigation to obtain access to classified information.


6 The FBI issued approximately 8,500 NSL requests in 2000, the year prior to passage of the USA PATRIOT Act. OIG Report, supra note 1, at vii.


10 Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).


13 David Pozen, The Mosaic Theory, National Security, and the Freedom of Informa-
The unitary executive theory posits unchecked power in the hands of the executive branch, beyond the oversight of Congress, the judiciary, or independent agencies. See e.g., Karl Manheim and Allan Ides, The Unitary Executive, 29 Los Angeles Lawyer, Sept. 2006, at 24.

Named for its chair, Senator Frank Church (Democrat from Idaho). Over 50,000 pages of Church Committee records have been declassified for public viewing. See Assassination Archives and Research Center, Church Committee Reports, available at www.aarclibrary.org/publib/church/reports/contents.htm (last visited Oct. 12, 2007) (listing the Church Committee Reports online). These records consist of the final reports issued by the Committee and transcripts of the hearings.

See generally Loch K. Johnson, A Season of Inquiry: Congress and Intelligence (1988).


RFPA, 92 Stat. at 3707.


Ibid. at 229 (referencing the additional views of Mr. LaFalce).


Compare ECPA, 100 Stat. at 1867, with RFPA Amendments, 100 Stat. at 3197.

ECPA, 100 Stat. at 1867.

RFPA Amendments, 100 Stat. at 3197.


ECPA, 100 Stat. at 1867; RFPA Amendments, 100 Stat. at 3197.


Ibid. at 36.


FCRA Amendments, 109 Stat. at 975.


The House passed the USA PATRIOT Act with a vote of 357 to 66, 147 Congressional Record H7224 (daily edition Oct. 23, 2001); the Senate voted 98 to 1, 147 Congressional Record S1059 (daily edition Oct. 25, 2001).


48 USA PATRIOT Act, Pub. L. No. 107-56, § 224, 115 Stat. 272 (2001). Some provisions set to expire included ECPA wiretapping (Sections 201, 202), sharing of foreign intelligence information (Section 203), roving wiretaps (Section 206), FISA wiretaps (Sections 207, 218), FISA pen register orders (Section 214), FISA access to business records (Section 215), and emergency disclosures by communications providers (Section 212).


54 Ibid. at 506.

55 Ibid. at 511.

56 Ibid. at 512.

57 Ibid.

58 Ibid. at 516.

59 Ibid. at 524.

60 Ibid. at 525–26.


63 Ibid. at 524.

64 Ibid. at 525–26.

65 Ibid. at 77.


67 Ibid. at 82.

68 Ibid.

69 Ibid.


National security letters


80 Ibid. §§ 118–119, 120 Stat. at 217–21. The first audit of NSL use required under PIRA Section 119 was released in March 2007. OIG Report, supra note 1.


82 AARA, § 5, 120 Stat. at 281.


84 Ibid. § 115, 120 Stat. at 211.

85 Ibid., 120 Stat. at 211–12.

86 Designated officials include the Attorney General, Deputy Attorneys General, Assistant Attorneys General, Director of the FBI, or the head or deputy head of a department or agency in the case of an FCRA NSL. Ibid., 120 Stat. at 212.

87 The court may still modify or lift a nondisclosure order if it determines such certification is made in bad faith. Ibid.

88 Ibid.

89 In addition to the persons listed supra note 86, other designated officials for recertified NSLs include designees of the Director of the FBI not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office. Ibid.

90 Doe I v. Gonzales, 449 F.3d 415, 449 (2d Cir. 2006).

91 Ibid.

92 Ibid.


100 Ibid. at 195.

101 Ibid. at 859.

102 Pozen, supra note 13, at 652 (stating that the Third Circuit has countenanced an abdication of mosaic theory review).

103 Ibid. (referring to the approach adopted by D.C. Circuit).

104 Ibid.

105 Ibid. at 637 (defining “standard deference” as the court “according substantial weight” to the executive’s national security judgments, but “without relinquishing its independent responsibility” to ensure that the executive’s decision is lawful).

106 Ibid. at 644 (discussing Muniz v. Meese, 115 F.R.D. 63 (D.D.C. 1987)).


108 Detroit Free Press v. Ashcroft, 303 F.3d 681 (6th Cir. 2002). But see N.J. Media Group, Inc. v. Ashcroft, 308 F.3d 198 (3d Cir. 2002) (also reviewing the “Creepy Directive” but deferring to the expertise of the government to determine whether closure of special interest cases is warranted).

109 Detroit Free Press, 303 F.3d at 710.


116 Ibid. at xxxiv.

117 Ibid.

118 Ibid.

119 Ibid. at xlvii.