



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 8 PVLR 13, 03/30/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### **National Security Letters: Practical Advice For Understanding and Handling Exceptional Requests**

By EDWARD R. McNICHOLAS

**N**ational Security Letters (“NSLs”) were once an exceptionally rare form of federal administrative subpoena that few corporate attorneys and privacy officers would ever confront. These statutes allow specified executive branch officials, without judicial oversight, to send a secret letter that requires the private recipient to produce specific types of information, including personal information about telecommunications subscriptions, toll records, financial records, and credit reports, without any notice to the data subjects.

In light of the U.S. response to international terrorism, the once infrequent use of NSLs and similar forms of process has increased significantly. For the four-year

period from 2003-2006, 192,499 formal requests for information were issued through NSLs.<sup>1</sup> Reports of the Department of Justice (“DOJ”) Inspector General, however, have sharply criticized the lack of effective controls on the use of NSLs, and civil libertarians have criticized both the government’s use of NSLs and companies that are believed to have honored them. The initial NSL report concluded that significant violations of NSL policies and procedures have occurred, and a later NSL report concluded that, while DOJ and the FBI had made “significant progress” in implementing the corrective actions, further improvements were still needed. Moreover, the report also described multiple instances of NSL recipients furnishing information beyond the scope of the NSL requests.

Regardless of whether a company regularly receives NSLs or receives one only in an exceptional case, the proper analysis and handling of such a request is significant for protecting national security, the company’s reputation, and the trust and confidence of customers. A failure to consider the constitutional, statutory and

*Edward R. McNicholas is a partner in the Privacy, Data Security and Information Law Group of the international law firm of Sidley Austin LLP and a member of BNA’s Privacy and Security Law Report Advisory Board. Previously, McNicholas served as an Associate Counsel to President Clinton. The views expressed herein are those of the author personally and do not necessarily reflect the views of any governmental or private entity, client, or association. This article is published for informational purpose only and is not legal advice. Readers should not act upon this article without seeking advice from professional advisers.*

<sup>1</sup> Public statistics on the use of NSLs and extensive background material are available in two lengthy reports by the Department of Justice’s (DOJ) Office of the Inspector General (OIG), on March 13, 2008, entitled A REVIEW OF THE FBI’S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, available at <http://www.usdoj.gov/oig/special/s0803b/final.pdf>, and on March 9, 2007, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS, available at <http://www.usdoj.gov/oig/special/s0703b/final.pdf>.

contractual rights of the data subjects and business partners can result in significant legal and/or business relationship exposure if the underlying investigation becomes public.

This article seeks to provide a legal primer that distinguishes the various forms of NSLs and related forms of legal process, summarizes the primary legal issues with their use including issues generated by European Union data protection laws, and then suggests some of the practical legal considerations that recipients need to address, both domestically and internationally.

**Varieties of National Security Letters.** Despite the general use of the term NSL to refer to any covert letter that compels the confidential provision of data to the U.S. government, the term NSL is merely a general reference for a small group of somewhat similar statutory authorities. Indeed, the statutory provisions do not even use the term “National Security Letter.” The unifying aspect of these provisions is that they effectively limit otherwise applicable statutory privacy protections and require the production of data, including personally identifiable information (often in a manner not contemplated by standard corporate privacy policies).

The scope afforded to NSLs is vast. Access is allowed to certain records that are merely relevant to “an authorized investigation to protect against international terrorism or clandestine intelligence activities.” NSLs thus authorize the seizure of records related to individuals who are not the specific target of a particular investigation, and the authorities do not necessarily require that the target of the NSL be a specified individual or group of individuals. Rather, as with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) investigation,<sup>2</sup> the NSL arguably can be aimed at an entire database of records that is relevant to “an authorized investigation to protect against international terrorism or clandestine intelligence activities.” 18 U.S.C. § 2709(b)(1). Because of their flexibility, NSLs often are used at the preliminary stages of investigations to establish links between people, corroborate potential theories, or generate the basis for even more intrusive searches, such as wiretaps.

The FBI is involved in the vast majority of NSLs, so effective constraints on the issuance of NSLs in large part depend on the FBI’s self-restraint, internal oversight, and professionalism. Internally, the DOJ requires that the FBI use NSLs only pursuant to the Attorney General’s Guidelines for National Security Investigations and Foreign Intelligence Gathering. Under the statutes and these guidelines, the FBI may issue NSLs if they are satisfied that the requirements are met. *First*, the FBI may access records only if an FBI official at least at the level of Special Agent in Charge makes the request. *Second*, the FBI must certify in writing that the records meet the threshold required under the relevant statutory authority. *Third*, as part of its evidentiary certification, the FBI must link the desired records to an authorized investigation. Oversight of this process is

<sup>2</sup> The SWIFT program reportedly involved the use of exceptionally broad administrative subpoenas, which may or may not have been NSLs, which resulted in the production of an entire database of records on international, inter-bank money transfers. NSLs are analyzed in the same way as administrative subpoenas, however, and so the administrative subpoenas in the SWIFT program are analogous, nomenclature notwithstanding.

provided by the DOJ, congressional committees, and an independent Inspector General who has investigated the internal controls over the use of these provisions. In addition, the President’s Privacy and Civil Liberties Oversight Board reviewed the use of NSLs, although that body has not had any members for several months.

The more particular legal restraints on NSLs are contained in specific provisions in four statutes under which the NSL is formally issued, each of which is discussed briefly. The four statutes are:

- ▶ Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2709, regarding telecommunications subscriber information, toll billing records information, and electronic communication transactional records;
- ▶ Right to Financial Privacy Act (“RFPA”), 12 U.S.C. § 3414, regarding financial records;
- ▶ Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681v and 15 U.S.C. § 1681u, regarding consumer credit reports and credit identity information; and
- ▶ National Security Agency Act, 50 U.S.C. § 436, regarding financial and travel information for individuals with access to classified information.

**The Electronic Communications Privacy Act** (“ECPA”) is one of the primary federal statutes protecting the privacy of electronic communications in the United States. ECPA is divided into two titles. Codified at 18 U.S.C. § 2510-2522, Title I of ECPA amended the Wiretap Act<sup>3</sup> and deals primarily with *ephemeral, real-time* communications. Codified at 18 U.S.C. § 2701-2712, Title II of ECPA, also known as the Stored Communications Act, concerns restrictions on access to *stored* electronic communications.

ECPA includes a significant NSL provision that authorizes electronic communications providers, in specified circumstances, to intercept communications and divulge their contents to the U.S. and to provide the federal government with calling records. As codified today, ECPA *requires* wire or electronic communications service providers to provide “name, address, length of service, and local and long distance toll billing records” based upon a certification that the records are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C. § 2709(b)(1). Significantly, the ECPA NSL provision cannot authorize government acquisition of the content of any communication or even the type of real-time telephone number information available under pen-trap orders.

**The Right to Financial Privacy Act of 1978** (“RFPA”), 12 U.S.C. §§ 3401-3422, generally protects customer records maintained by covered financial institutions from improper disclosure to officials or agencies of the federal government; it is the public sector counterpart of private sector financial privacy restrictions. Under RFPA, unless an exception applies, a govern-

<sup>3</sup> More precisely, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 was amended by Title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848. It is codified at 18 U.S.C. §§ 2510-2522 and known together as “The Wiretap Act.”

ment authority may have access to or obtain copies of the information contained in the financial records of any customer of a covered financial institution only through specified methods that generally involve notice to the customer whose records are sought, as well as a “waiting period” during which the customer may challenge the disclosure. *See id.* §§ 3402, 3410.<sup>4</sup>

Since 1978, however, RFPA also has contained accommodations for special governmental access to financial records. Under section 3414, special procedures are applicable to the disclosure of financial records (i) requested by government authorities for intelligence purposes, (ii) requested by the FBI, and (iii) requested in emergency situations. Beyond these special procedures, exemptions allow voluntary disclosures of potential illegal activity to the government, *id.* § 3403(c), disclosures to grand juries, *id.* § 3413(i), and disclosure of limited “locator” information, *id.* § 3413(g).

The current version of RFPA allows further special procedures, particularly with respect to two areas—intelligence investigations and FBI investigations. With respect to intelligence investigations, RFPA contains a general exemption for “the production and disclosure of financial records pursuant to requests from . . . a Government authority authorized to conduct investigations of, or intelligence or counterintelligence of analyses related to, international terrorism for the purpose of conducting such investigations or analyses.” *Id.* § 3414(a)(1)(C). With respect to FBI investigations, section 3414(a)(5) includes special NSL procedures for the FBI to obtain records.<sup>5</sup> According to those procedures, financial institutions “shall comply” with a request for a customer’s or entity’s financial records “sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment of the Constitution of the United States.” *Id.* § 3414(a)(5)(A).

**The Fair Credit Reporting Act** (“FCRA”), 15 U.S.C. § 1681v and 15 U.S.C. § 1681u, also is related to financial privacy and was enacted in 1970 to ensure accuracy and fairness in credit report information about consumers. Basic “credit header” information generally has been available to law enforcement from any of the credit reporting agencies. Pursuant to NSL authority, the FBI also has the ability to access full credit reports in the course of an authorized intelligence, counterintelligence, or international terrorism investigation. Sig-

nificantly, the authority at § 1681(v) extends beyond the FBI to any “government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism.”

**The National Security Act**, 50 U.S.C. § 436, is perhaps the most obscure of these authorities, and provides for NSL authority to access financial and travel information in circumstances where the government investigates a current or former employee’s use of or access to classified information. This authority also extends to “[a]ny authorized investigative agency,” which is considerably broader than the FBI.

**Related Forms of Federal Process.** The federal government has a broad range of other mechanisms to compel production of information, including court orders, grand jury subpoenas, administrative procedures, foreign intelligence collection authorities, and specific authorities contained within statutes governing the collection of particular types of information. Traditionally, grand jury subpoenas have been the most common method used by the U.S. government to acquire personal information in the context of criminal investigations, and they have enjoyed unique secrecy restrictions deemed necessary to protect the independence of the grand jury process from inappropriate influences. NSLs, however, have been used in circumstances where even the secrecy of the grand jury subpoena is deemed inadequate, or when a grand jury has yet to be empanelled.

NSLs, however, should be distinguished from less formal requests from the federal government for assistance with criminal or intelligence matters. Although agencies other than those specified in the NSL statutes could make a request that a company assist with a matter of national security, a voluntary request could have a significantly different legal analysis. Such requests do not appear to have any specific statutory basis, and there is essentially no specific case law directly on point regarding such requests.<sup>6</sup>

**Restrictions on Recipients.** Recipients of NSLs or similar requests face legal restrictions on the disclosure of even the existence of the request. Some of the initial NSL authorities suggested that not even legal counsel could be consulted, and the NSL read literally could ask the recipient, who may be a chief information officer or branch manager, to provide data without informing su-

<sup>4</sup> A financial institution normally is not allowed to release financial records of a customer until the government authority certifies compliance in writing to the financial institution. 12 U.S.C. § 3403(b). In addition, a financial institution (including its officers, employees and agents) is prohibited from providing a government authority access to, copies of, or information contained in, the financial records of a customer, except in accordance with the applicable provisions of the statute. *Id.* § 3403(a). Note that RFPA uses several definitions of “financial institution.”

<sup>5</sup> While RFPA does not refer to “National Security Letters,” certificates issued pursuant to this section are generally considered to be NSLs because they affirmatively grant the FBI covert access to financial records. *See also* USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177 (H.R. 3199), 120 Stat. 192 (2006) (referring to requests under this section as “National Security Letters”).

<sup>6</sup> It is also significant to distinguish the very rare so-called “Section 215 Orders.” Section 215 of the USA PATRIOT Act amended the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1812 (“FISA”), to establish a procedure that broadened existing authority allowing the Director of the FBI (or specified designees) to apply for court orders compelling disclosure of *business records* where the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. *Id.* § 1861. Significantly, the provision also created immunity for the business complying in good faith with the orders and required certain reporting to Congress. The practical significance of this unusual provision has been overstated, however, largely due to disproportionate media attention and because “Section 215 Orders” are court orders. The DOJ Inspector General, after an independent review, reported that, from 2002 to 2005, only 21 total applications (regarding 18 unique requests) were submitted under this authority.

pervisors or consulting legal counsel. The legal restrictions against seeking outside legal advice have been removed, but NSLs retain onerous restrictions for corporate recipients.

*First*, NSL provisions directly prohibit any person from disclosing even “the existence” of the surveillance activities “with respect to which the person has been furnished a court order or certification,” and “[a]ny such disclosure shall render such person liable for” civil damages. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(ii) (ECPA provision). *Second*, “any information with respect to the activities” of the National Security Agency is protected from disclosure by Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note, which provides that “nothing” in “any” law can override the authority and responsibility of the Director of National Intelligence to protect such information from disclosure). *See Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996) (considering this protection “by its very terms, absolute”). *Third*, it is a felony to disclose any classified information that is involved, and NSLs can be classified documents. *See, e.g.*, 18 U.S.C. § 798(a).

**Constitutional Challenges to NSL Authorities.** In assessing the legal risk presented by compliance with NSLs, it is important to note that NSLs have not been tested in the courts on the core Fourth Amendment issues, apparently because the government has a practice of mooting such challenges by withdrawing the NSL.<sup>7</sup> Only a few cases involving NSLs are known to exist, and on the key Fourth Amendment issues, these cases have essentially established only that NSLs are analyzed like administrative subpoenas.

It is clear that the ability of data subjects to challenge disclosure of their own information under NSL provisions is very limited. Provisions governing NSLs generally address records about individuals held by third parties, and, academic criticism of this rule notwithstanding, the Supreme Court has held that individuals do not possess Fourth Amendment rights in financial and transactional records in the possession of a third party. *See, e.g., United States v. Miller*, 425 U.S. 435 (1976). Rather, the privacy protection afforded such data arises from statutes, which generally do not contain provisions allowing third party challenges to the collection of information, including information about such third parties.

In *Doe v. Holder*, No. 07-cv-4943 (2d Cir.), the ACLU is pursuing a suit challenging the constitutionality of the ECPA NSL provision.<sup>8</sup> The district court initially

held the provision to be facially unconstitutional. *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004). After an appellate remand, the U.S. Court of Appeals for the Second Circuit recently held that section 2709(c) and the NSL judicial review statute (section 3511) are unconstitutional violations of the First—not Fourth—Amendment, to the extent they impose a nondisclosure requirement on NSL recipients without placing on the government the burden of initiating judicial review of such a requirement. *Doe Inc. v. Mukasey*, 549 F.3d 861, 874-81 (2d Cir. 2008). In dicta, however, the court suggested that the government could satisfy this burden by requesting notice from the NSL recipient of their intent to contest the non-disclosure requirement. *Id.* at 879. The court also held that section 3511 is unconstitutional to the extent that it allows conclusive weight to a government official’s certification that there must be non-disclosure to avoid endangering national security or interfering with diplomatic relations. *Id.* at 881-84. The court modified the existing injunction so that it now only enjoins FBI officials from enforcing the non-disclosure provision in the absence of government-initiated judicial review. *Id.* at 885. Existing ECPA NSLs, however, continue to be valid, and compliance remains mandatory.

**Immunity and Compliance Challenges.** NSLs traditionally were both informal and rare. The statutes did not specify a deadline for compliance, and, until 2006, the government had no clear authority to enforce the NSL if the recipient simply refused to comply.

Nonetheless, even before the 2006 amendments, if a facially-valid NSL was received and followed, the recipient would enjoy broad immunity for actions taken in good faith under U.S. law (as well as preemption of any contrary state law). Absent particular statutory restrictions, corporations disclose their own business records in response even to informal government requests, unless their contracts or customer agreements promised otherwise.

Under current law, NSLs can be challenged under the legal standards of the unified provision for their judicial review at 18 U.S.C. § 3511. Under the provision, NSLs can be quashed or modified when compliance would be “unreasonable, oppressive, or otherwise unlawful.” § 3511(a). Under section 3511(c), the Attorney General may also now bring an action in federal district court to compel compliance. If compliance is ordered by the court, any failure to obey would be punishable as contempt of court.

Companies receiving NSLs retain privacy interests that have been judicially recognized as adequate to

<sup>7</sup> The Fourth Amendment to the United States Constitution guarantees the context-specific analysis of reasonableness under the circumstances so as to avoid “unreasonable searches and seizures.” U.S. CONST. amend. IV.

<sup>8</sup> In what was originally *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (3 PVL 1127, 10/4/04), vacated sub nom. *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (per curiam) (5 PVL 769, 5/29/06), a district court addressed a constitutional challenge to an NSL brought by an Internet service provider (“ISP”) which had been served with an ECPA NSL under 18 U.S.C. § 2709. In denying a motion to dismiss, the court found that the NSL violated the Fourth Amendment because of the blanket non-disclosure rules in place at the time and the absence of judicial review. *Id.* at 506. In doing so, the court considered NSLs to be “a unique form of administrative subpoena,” *id.* at 475, and found that the Fourth Amendment pri-

vacuity interest at issue belonged to the ISP, not its customers. *Id.* at 494 n.118. In a companion case on appeal, *Doe v. Gonzales*, another district court focused on the First Amendment issues raised by the complete non-disclosure rules, 386 F. Supp. 2d 66 (D. Conn. 2005) (4 PVL 1148, 9/19/05). Subsequently, however, the USA PATRIOT Act reauthorization statutes – Pub. L. No. 109-177, 120 Stat. 192 (H.R. 3199) and Pub. L. No. 109-178, 120 Stat. 278 (2006) (S. 2271)—amended the NSL statutes to provide for judicial enforcement of NSLs and their nondisclosure requirements. Due to these subsequent amendments to the non-disclosure rules, both of the prior decisions regarding these provisions were vacated and dismissed as moot on appeal. *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (per curiam) (5 PVL 769, 5/29/06). The challenges, however, have continued.

challenge NSLs. These privacy interests do not stem from the data subject's right in their personal information, however, so that the individual with the most interest in challenging a particular NSL is almost always entirely unaware of its existence. Rather, current law recognizes only the interests of the entity receiving the order in the privacy of its own business records, as the S.D.N.Y. explained:

To be clear, the Fourth Amendment rights at issue here belong to the person or entity receiving the NSL, not to the person or entity to whom the subpoenaed records pertain. Individuals possess a limited Fourth Amendment interest in records which they voluntarily convey to a third party.

*Doe v. Ashcroft*, 334 F. Supp. 2d at 494 n.118. The United States Foreign Intelligence Surveillance Court of Review recently released a significant decision essentially recognizing corporate rights to challenge covert legal process.<sup>9</sup> Thus, the ability to challenge governmental requests frequently rests with the data processor—not with the data subject—although the data processor may have bound itself in its privacy policy, terms of use, or otherwise as a matter of contract to contest an order. Indeed, perhaps the most direct risk regarding NSLs would be the potential for breach of contract actions by business partners, consumer actions based on violations of privacy policies, or other public interest litigation. Even if litigation were unsuccessful, customer relations and branding may be harmed if compliance is deemed excessive by consumers.

When challenged as “unreasonable, oppressive, or otherwise unlawful,” NSLs are likely to be limited by a requirement that they reasonably describe the records sought and not be so broad as to offend traditional Fourth Amendment principles. *Cf. Theofel v. Farley-Jones*, 359 F.3d 1066, 1071-72 (9th Cir. 2004) (3 PVL 247, 3/1/04) (considering a subpoena for “[a]ll copies of e-mails sent or received by anyone” at a specified company to be “‘on its face . . . massively overbroad’” and “‘patently unlawful’” and “‘transparently and egregiously’” in violation of the federal rules). The scope of information requested by NSLs presents one of the most significant issues for a recipient. An NSL requesting specific information about a particular person would obviously pose different litigation exposure than an NSL requesting, as in the SWIFT case, a copy of all transactions in a database. The USA PATRIOT Act, however, lowered the evidentiary threshold to issue an NSL by allowing access to any record “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.” 18 U.S.C. § 2709(b)(1) (emphasis added). As a result, the government may obtain records of individuals who are not the specific relevant target of a particular investigation and may justify extensive data requests potentially

<sup>9</sup> See *In re Directives*, 551 F.3d 1004 (Foreign Intel. Surv. Ct. of Rev. 2008) (upholding the constitutionality of certain directives issued to an unidentified communications provider under the now-superseded Protect America Act). Although that court rejected a telecommunications carrier's Fourth Amendment challenge to an order under an amendment to FISA, the Court did recognize the carrier's standing. Significantly, the Court also held that the Fourth Amendment allows warrantless surveillance undertaken for national security purposes if it is “reasonable” under a “totality of the circumstances” test. *Id.* at 1012.

useful for data mining activities, such as the requests made for the SWIFT database. Indeed, although the matter was eventually dismissed, a U.S. federal court considering privacy challenges to the SWIFT program expressed significant concerns with the program and declined to dismiss a privacy complaint against SWIFT.<sup>10</sup>

Courts have provided little guidance on the issue of when an NSL would constitute an unlawful search, in part because the United States has mooted every known attempt to mount a Fourth Amendment challenge to an NSL. Arguably, however, the court in the vacated S.D.N.Y. decision cited above suggested some limits on NSLs by analogizing them to administrative subpoenas and thereby potentially adopting a Fourth Amendment “reasonableness” standard for their scope. As that court explained, however, an administrative subpoena needs only to be “reasonable,” which the U.S. Supreme Court has interpreted to mean that “(1) the administrative subpoena is ‘within the authority of the agency;’ (2) that the demand is ‘not too indefinite;’ and (3) that the information sought is ‘reasonably relevant’ to a proper inquiry.” *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 495 (S.D.N.Y. 2004) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950)), *vacated sub nom on other grounds Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (*per curiam*) (5 PVL 769, 5/29/06). Even this modest limit on the scope of NSLs, however, is essentially untested in the courts.

**Practical Domestic Data Protection Considerations.** The most important practice tip regarding NSLs is to publish in advance a policy regarding their handling. NSLs can be served on contacts outside of the general counsel's office, and, particularly in light of the secrecy involved with NSLs and their somber boilerplate provisions, NSLs can reach the general counsel's office only after compliance, if at all. Privacy officers and general counsels need to make their views about the responses to NSLs known in advance and to require their inclusion in formulating the response. NSLs certainly should be subject to close-hold handling, so the privacy officers and general counsels could be closed out of that loop unless policies require their approval prior to the NSL response.

Such policies should focus attention on the skilled review of the NSL to ensure that it contains language to make it legally binding and to protect the company. Moreover, it is important that the recipient agree that the scope and scale of the request is reasonable and that any business partner or consumer privacy policy issues are addressed. In particular, if the recipient is handling data on behalf of another entity, it will be important to review any contractual privacy commitments that govern that data. Likewise, any relevant representations in a privacy policy must be considered.

Although NSLs are mandatory, recipients who regularly receive them may also be able to negotiate with the agency in interest to reduce the associated burden, to provide further assurances from the government, and to

<sup>10</sup> See *Walker v. SWIFT SCRL*, 491 F. Supp. 2d 781 (N.D. Ill. 2007) (6 PVL 1007, 6/25/07) (largely denying SWIFT's motion to dismiss); see also *Walker v. SWIFT SCRL*, No. 06C3447 (N.D. Ill. June 12, 2007) (order transferring case to Eastern District of Virginia); *Walker v. SWIFT SCRL*, 517 F. Supp. 2d 801 (E.D. Va. 2007) (dismissing action).

allow for legal review. In particular, the government's unwillingness to litigate the core Fourth Amendment viability of NSLs can create potential leverage for recipients who are willing to challenge the NSL. Given the confidentiality surrounding NSLs, however, such negotiations are often classified or, at least, highly confidential.

**Foreign Law Exposure.** Regardless of U.S. law, foreign laws concerning personal data, such as in the European Union, also pose risk for companies with international customers or operations. The most prominent concern would arise under the European Union Data Protection Directive (95/46/EC) (the "Directive")<sup>11</sup> and related EU Member State legislation.<sup>12</sup> In particular, high profile EU cases involving Sarbanes-Oxley Act whistle-blower hotlines and the SWIFT Inter-bank funds transfer system have made clear that EU jurisdictions may not always respect a foreign compulsion of law defense, which means that EU laws could still be violated even if mandatory legal process is obtained in the United States. In its opinions in both the SWIFT and SOX matters, the EU Article 29 Data Protection Working Party expressly noted that "'an obligation imposed by a foreign legal statute or regulation . . . may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate.'" <sup>13</sup>

With respect to both the SWIFT and Sarbanes-Oxley situations, however, the EU DPA's have not assessed fi-

nancial penalties, but have rather written opinions critical of the relationship and then sought to negotiate enhanced privacy protections. Significantly, when the SWIFT program became public, the U.S. Treasury Department made clear that SWIFT was merely complying with administrative subpoenas (similar to NSLs) to provide databases, that there were significant limitations on the types of queries made in those databases, and that there was independent auditing of queries actually made of the databases in the classified setting. Even these protections, however, were deemed inadequate by multiple DPAs. Later DPAs have considered the program to provide adequate safeguards under EU law, but the end result of the controversy was a significant amount of brand damage, substantial legal fees, and a negotiated withdrawal of the servers from U.S. territory to avoid being subject to mandatory U.S. legal process, at a total cost estimated at \$200 million (although there is some suggestion that the movement of the servers was also motivated in part by business purposes).

The United States and European Union, however, have been attempting to negotiate an agreement on data transfer with respect to criminal investigations, and the "High-Level Contact Group" appears to have reached some agreement on general principles for criminal investigation sharing. Precisely how this agreement will affect NSLs, however, remains to be seen once the agreement is finalized.

#### **Practical Trans-Border Data Protection Considerations.**

In formulating an NSL policy that involves transborder flow of data, it is important to keep in mind the corporate structure at issue. A troublesome scenario involves an attempt by a U.S. government authority to obtain records held by a subsidiary of a U.S. company, where the subsidiary is located outside the U.S. These concerns are particularly pronounced when the subsidiary holds the records merely as a data processor for a foreign company. The U.S. has vigorously asserted extraterritorial jurisdiction over activity outside the United States where "conduct outside its territory . . . has or is intended to have substantial effect within its territory."<sup>14</sup>

Constructing contractual provisions to limit the potential disclosure of information to the U.S. government by international data processing subsidiaries is a complex issue that is highly dependent on the particular context addressed by the contract, the protections sought (e.g., notice to the data controller or subject, compared to non-disclosure), and the types of contemplated U.S. government process. Even so, appropriate contracts may be an important part of a data security strategy, and they may be essential for U.S. companies seeking to reassure foreign clients.

A broad prohibition against disclosure in the data controller's contracts, however, would likely be ineffective in many cases in light of the compulsory nature of

<sup>11</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

<sup>12</sup> The Directive imposes obligations on Member States, who must implement the principles of the Directive in their national laws. These national laws in turn impose direct obligations on the individuals and entities to whom they apply. Under the Directive, each Member State must provide for the right of every person to a judicial remedy for any breach of his or her rights under the national data protection laws implementing the Directive, *see* Article 22, for entitlement to compensation from the data controller in case of damage suffered as a result of any act incompatible with such legislation, *see* Article 23, and for sanctions in case of infringement of such legislation, *see* Article 24. In addition, the Directive requires Member States to provide that one or more public authorities be responsible for monitoring the application of the national legislation implementing the Directive. *See* Article 28(1). In particular, these Data Protection Authorities ("DPAs") must be endowed with investigative powers, effective powers of intervention, and the power to engage in legal proceedings where the national provisions implementing the Directive have been violated, or to bring these violations to the attention of the judicial authorities. *See* Article 28(3). Further, the national DPAs shall hear claims lodged by any person concerning the protection of his or her data protection rights. *See* Article 28(4).

<sup>13</sup> Article 29 Data Protection Working Party, 01935/06/EN, WP 128, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* 17-18 (Nov. 22, 2006), available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp128\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf) (emphasis omitted) (quoting Article 29 Data Protection Working Party, 00195/06/EN, WP 117, *Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime* 8 (Feb. 1, 2006), available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp117\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf)).

<sup>14</sup> RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1) (1987). Not surprisingly, after September 11, 2001, U.S. courts have deemed international terrorism as having sufficiently "substantial effects" within the U.S. to justify the limited extraterritorial application of the USA PATRIOT Act. *See, e.g. Tzvi Weiss v. Nat'l Westminster Bank*, 242 F.R.D. 33 (E.D.N.Y. 2007) (ordering U.K. bank to produce financial records); *Strauss v. Credit Lyonnais*, 242 F.R.D. 199 (E.D.N.Y. 2007) (ordering French bank to produce financial records).

---

NSLs. Nonetheless, sophisticated corporations often can provide foreign data controllers with a range of assurances against disclosure of their data by service providers owned by U.S. companies. Measures shaping the corporate structure may be successful in certain respects if they provide the foreign data processor with sufficient independence from the U.S. affiliate. Moreover, data controllers can enhance control of their data while it is in the possession of foreign data processors by adding specific restrictions in the contracts of its foreign-affiliated service providers. Even where such provisions may not entirely bar the U.S. government

from access to the personal data, they may assist in negotiations regarding the scope of such a request, informal efforts to resolve the matter short of litigation, and scrutiny of the issue by an independent judicial officer in the United States or in a foreign court if the matter is ever disclosed or forced into litigation.

Ultimately, the practical significance of NSLs will depend upon the uses of them made by the new Obama-Biden Administration. There has been no change in the need to protect against international terrorism, however, and so NSLs may well remain a significant weapon in that fight.