Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Patriot Act And The Cloud: Part 1

Law360, New York (January 23, 2012, 1:23 PM ET) -- President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 into law on Oct. 26, 2001, in the wake of the 9/11 terrorists attacks on New York City and the Pentagon. The stated purpose of the Patriot Act is "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[1] It is one of the most controversial, polarizing and, in many respects, misunderstood, pieces of U.S. legislation this century.

In the cloud context, European consumers, among others, have expressed concern that the Patriot Act will afford the U.S. government undue and unfettered access to their data if they choose to store it in the cloud servers of U.S. providers, such as Microsoft Corp. or IBM Corp.[2] A recent survey found that 70 percent of Europeans have concerns about their online data and how well it is secured.[3]

For many, these fears were exacerbated by an announcement by Gordon Frazer, the managing director of Microsoft U.K., that he could not guarantee that data stored on Microsoft servers, wherever located, would not end up in the hands of the U.S. government, because Microsoft, a company based in the United States, is subject to U.S. laws, including the Patriot Act.[4]

"It is crucial, for European businesses and users, that the data on the cloud is stored in a safe country," said Philippe Juvin, a member of the European Parliament.[5] Aware of these concerns, some EU data centers have gone so far as to advertise that they provide "'a safe haven from the reaches of the U.S. Patriot Act.'"[6]

To evaluate the validity of these concerns, several questions must be considered. First, what information, exactly, does the Patriot Act reach? Second, how likely is it, as a practical matter, that the Patriot Act will ever be used to reach a European company's data stored in the cloud? Finally, how does that risk compare with exposure that European companies already face, such as the prospect of their home country governments accessing their cloud-stored data?

As Ambassador Phillip Verveer, the U.S. State Department's coordinator for international communications and information policy, explains, "The PATRIOT Act has come to be a kind of label for [privacy] concerns. We think, to some extent, it's taking advantage of a misperception, and we'd like to clear up that misperception."[7]

This two-part article aims to dispel some of the myths shrouding the Patriot Act, and to provide an assessment of the risks the Patriot Act poses to data stored in the cloud, particularly where the data, or its owner, are based outside of the United States.

Patriot Act Discovery Tools for Law Enforcement

Although — contrary to a common misconception — the Patriot Act did not create entirely new procedural mechanisms for U.S. law enforcement to use to obtain data in furtherance of its investigations, the Patriot Act did expand certain discovery mechanisms already available to U.S. law enforcement. Two such tools that U.S. law enforcement could use to access data in the cloud — Foreign Intelligence Surveillance Act orders ("FISA orders") and National Security Letters — warrant discussion. Both were materially enhanced by, and especially controversial in the wake of, the Patriot Act.

FISA Orders

Prior to enactment of the Patriot Act, the Foreign Intelligence Surveillance Act permitted the FBI to apply to a special court, the Foreign Intelligence Surveillance Court, to obtain a FISA order that would allow the FBI to obtain the business records of third parties for foreign intelligence and international terrorism investigations.[8] Such business records, however, originally were limited to car rental, hotel, storage locker and common carrier records.

Title II of the Patriot Act, Enhanced Surveillance Procedures, expanded the reach of FISA orders to allow the FBI to obtain any type of business records, specifically providing in Section 215 that the FBI can apply to a judge or magistrate judge of the Foreign Intelligence Surveillance Court for "an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[9]

This provision has been read to include "floppy disks, data tapes, computers and their hard drives, and any type of record in any format."[10] Thus, this includes data in the cloud. To obtain a FISA order, the FBI must specify that the tangible things sought are for an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism and clandestine intelligence activities. Section 215 specifies that FISA orders may not be based on investigations of U.S. persons founded solely on conduct by such persons that is protected by the First Amendment of the U.S. Constitution.

FISA orders, particularly as expanded under Section 215 of the Patriot Act, have given rise to privacy concerns for several reasons. First, such orders may be granted ex parte, meaning with only the FBI, and no other party, presenting evidence to the court.

Second, purportedly for the purpose of avoiding compromising ongoing investigations, Section 215 includes a "gag" provision that prohibits the party that receives a FISA order from disclosing that fact, subject to certain limited exceptions such as to receive legal advice. This typically would prevent a cloud service provider from informing its customers that the service provider had shared their data with the FBI in response to a FISA order.

Third, the fact that Section 215 allows the FBI to obtain a person's library records sparked significant protests that the provision was invasive of basic civil liberties and reader privacy, and in fact led Section 215 commonly to be referred to as the "library records" provision.[11]

Finally, the American Civil Liberties Unions objects that "[t]he FBI need not show probable cause, nor even reasonable grounds to believe, that the person whose records it seeks is engaged in criminal activity."[12] "Probable cause" is generally considered the minimum showing necessary for law enforcement to conduct a search consistent with the protections against unreasonable searches and seizures set forth in the Fourth Amendment to the U.S. Constitution.

In the USA Patriot Act Improvement and Reauthorization Act of 2005, enacted March 9, 2006, Congress took several steps to address these concerns. First, any request for library, tax or firearms records now must be approved by the director of the FBI or one of two senior FBI officers. Second, the recipient of a Section 215 order now has an express right to oppose the order and to be heard promptly by the Foreign Intelligence Surveillance Court.

Third, an application must include a "statement of facts" demonstrating that there are reasonable grounds to believe that the tangible things sought are "relevant" to an authorized or preliminary investigation to protect against international terrorism or espionage, or to obtain foreign intelligence information not concerning a U.S. person.[13]

Fourth, the gag provision also can be contested before the Foreign Intelligence Surveillance Court by the party receiving the FISA order, but only after a year. Fourth, Congress required the U.S. attorney general to promulgate regulations to "minimize the retention, and prohibit the dissemination, of non-publicly available information" obtained with a FISA order, in a manner "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." Notwithstanding these efforts, privacy and civil liberties advocates remain deeply troubled by Section 215.

What is the practical effect of FISA orders on users of U.S. cloud services? The answer is that the FBI rarely uses FISA orders. In 2010, the U.S. government made only 96 applications to the Foreign Intelligence Surveillance Courts for FISA orders granting access to business records.[14] Of those requests, 80 percent were for Internet records.[15] There are several reasons why the FBI may be reluctant to use FISA orders: public outcry; internal FBI politics necessary to obtain approval to seek FISA orders; and, the availability of other, less controversial mechanisms, with greater due process protections, to seek data that the FBI wants to access.

As a result, this Patriot Act tool poses little risk for cloud users. With such a small number of FISA orders for business records sought, and such orders being limited to data that the FBI believes relates to a terrorism or espionage investigation, the FISA order risk is more theoretical than practical.

National Security Letters

The national security letter ("NSL") is a form of administrative subpoena that the FBI and other U.S. government agencies can use to obtain certain records and data pertaining to various types of government investigations. NSLs first arose as an exception to the Right to Financial Privacy Act of 1978 ("RFPA").

The RFPA allowed — but did not require — financial institutions to disclose customer financial records to (1) government intelligence agencies for intelligence uses and (2) the Secret Service for use in its protective activities.[16] The RFPA also included a gag provision, prohibiting financial institutions and their officers who had received NSLs from disclosing that fact. Subsequent legislation continued to expand upon NSL authority. In 1986, financial institution compliance with NLSs become mandatory.[17]

By the time the Patriot Act was enacted, there were already four federal statutes authorizing enumerated government authorities (chiefly the FBI) to issue NSLs to obtain certain specifically enumerated types of data from certain specifically enumerated third parties. First, as noted above, under the RFPA, the FBI or the Secret Service may obtain financial records from financial institutions[18] such as banks, securities brokerages, car dealers, pawn brokers, casinos and real estate agents, among others (accountants and auditors, however, are not included).[19]

Second, under the Fair Credit Reporting Act, the FBI may use a NSL to obtain from a consumer reporting agency the names and addresses of all financial institutions at which a consumer maintains or has maintained an account, plus consumer identifying information such as name, address and employment history.[20]

For these purposes, the term "consumer reporting agency" means any person which regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. This definition would include the three major credit bureaus (TransUnion, Equifax, Experian) and other similar entities.

Third, under the Electronic Communications Privacy Act, the FBI may request, from wire or electronic service providers (including Internet service providers) subscriber information, toll billing records information and electronic communication transactions records.[21] The U.S. Department of Justice takes the position that this includes, with regard to e-mail accounts, the name, address and length of service of a person, as well as e-mail addresses associated with an account and screen names.[22]

Fourth, under the National Security Act, an authorized government investigative agency may request any of the types of information described above, from any of the sources described above, when necessary to conduct security checks of government employees or investigate U.S. government employees believed to be spying for foreign powers.[23]

Title V of the Patriot Act, Removing Obstacles to Investigating Terrorism, expanded the foregoing provisions in several respects. As for most sections available to the FBI (the RFPA, Fair Credit Reporting Act and the Electronic Communications Privacy Act), Section 505 of the Patriot Act expanded the FBI's authority to make NSL requests beyond its headquarters, to its 56 field offices.[24]

Section 505 also eliminated the requirement that information sought relate to a foreign power or an agent of foreign power, instead substituting a lower standard, requiring that the NSL request be relevant to international terrorism or foreign spying. Section 505 also allowed the FBI to obtain full consumer credit reports.[25]

Section 358(g) of the Patriot Act added yet another NSL section to the Fair Credit Reporting Act, this one allowing not just the FBI, but any government agency, to obtain information from a consumer reporting agency in connection with international terrorism or intelligence activities.

After the Patriot Act expanded the scope of NSLs as described above, their use began to rise, from 8,500 NSLs in 2000 to between 39,000 to 49,000 per year from 2003 and 2006.[26] The Department of Justice reported to Congress that, in 2010, the FBI made 24,287 NSL requests (excluding requests for subscriber information only) for information concerning 14,212 U.S. persons.[27]

NSLs give rise to privacy concerns and, according to critics, the potential for abuse, for several reasons. First, as noted above, the Patriot Act expanded the universe of government agencies that can use NSLs. For example, The New York Times has reported that the Pentagon and the CIA have used NSLs.[28] Second, the FBI may issue NSLs on its own initiative, without the authorization of any court. (This was true even before the Patriot Act.)

Typically, the only requirement under the Patriot Act is that the FBI provide a written certification, from its director or a senior designee in its head office or a field office, that the information sought is necessary to protect against international terrorism or clandestine intelligence activities.

Nothing in the Patriot Act provides for any judicial review of the FBI's decision to issue an NSL. The Patriot Act imposes similar written certification requirements on other government agencies that are permitted to use NSLs, and similarly lacks a procedure for judicial review.

Third, the NSL statutes impose a gag requirement on persons receiving an NSL, thereby prohibiting recipients from disclosing the fact that they have received an NSL. In addition, the Attorney General Guidelines and various information-sharing agreements require the FBI to share NSL information with other federal agencies and the U.S. intelligence community.[29]

In Doe v. Ashcoft, a federal court in New York concluded that the NSL statutes were unconstitutional as written. The court, looking at one of the statutes (18 U.S.C. § 2709), concluded that it was unconstitutional under the Fourth Amendment because "in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process."[30]

As well, the court concluded that the NSL provisions violated the First Amendment because its gag order provisions apply "in every case, to any person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected, under any circumstances, either by the FBI itself, or pursuant to judicial process."[31]

Thereafter, the 2005 Patriot Act Reauthorization Act tried to redress some of these concerns. It provided a right to judicial review of NSLs, affording recipients the right to petition a federal court for an order modifying or setting aside the NSL, and granting federal judges the authority to modify or set aside the NSL if compliance would be unreasonable, oppressive, or otherwise unlawful.

The Reauthorization Act also provided recipients with a right to petition the court to lift the gag order — but there, the burden on the petitioner is much higher. If the FBI (or other government agency) certifies that the gag order is necessary to protect national security or diplomatic relations, then that certification is conclusive unless it was issued in bad faith. The Reauthorization Act also provided criminal penalties for violating gag obligations with the intent to obstruct an investigation.

So where does this complex statutory scheme leave cloud users? While the use of NSLs is not uncommon, the types of data that U.S. authorities can gather from cloud service providers via an NSL is limited. In particular, the FBI cannot properly insist via NSLs that Internet service providers share the content of communications or other underlying data.

Rather, as set forth above, the statutory provisions authorizing NSLs allow the FBI to obtain "envelope" information from Internet service providers. Indeed, the information that is specifically listed in the relevant statute is limited to a customer's name, address, and length of service. The FBI often seeks more, such as who sent and received emails and what websites customers visited. "But more recently, many service providers receiving national security letters have limited the information they give to customers' names, addresses, length of service and phone billing records."[32]

"'Beginning in late 2009, certain electronic communications service providers no longer honored' more expansive requests, FBI officials wrote in August [2011], in response to questions from the Senate Judiciary Committee."[33]

Although cloud users should expect their service providers who have a U.S. presence to comply with U.S. law, users also can reasonably ask that their cloud service providers limit what they share in response to an NSL to the minimum required by law. If cloud service providers do so, then their customers' data should typically face only minimal exposure due to NSLs.

--By Alex C. Lakatos, Mayer Brown LLP

Alex Lakatos is a partner in Mayer Brown's financial services regulatory and enforcement group, in the firm's Washington, D.C., office.

The author wishes to thank Kelly B. Kramer, a partner in the firm's white collar practice in Washington, and Rebecca S. Eisner, a partner in Mayer Brown's outsourcing practice in the firm's Chicago office, for their assistance with this article.

[1] The text of the Patriot Act is available online at http://epic.org/privacy/terrorism/hr3162.html.

[2] Sean Gallagher, PATRIOT Act and privacy laws take a bite out of US Cloud Business, ARS Technica (Dec. 8, 2011, 7:49 AM), http://arstechnica.com/tech-policy/news/2011/12/patriot-act-and-privacy-laws-take-a-bite-out-of-us-cloud-business.ars.

[3] Jennifer Baker, Europe cloud vendors cleaning up with data protection fears US vendors compromised by lax privacy laws, claim European firms, IDG News (Dec. 5, 2011, 10:14 AM), http://news.techworld.com/security/3322757/europe-cloud-vendors-cleaning-up-with-data-protection-fears/.

[4] Zack Whittaker, Microsoft admits Patriot Act can access EU-based cloud data, ZDNet (June 28, 2011, 8:10 AM PDT), http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225?tag=content;siu-container.

[5] Baker, supra note 3.

[6] Baker, supra note 3.

[7] David Saleh Rauf, PATRIOT Act clouds picture for tech, Politico (Nov. 29, 2011, 11:17 PM EST), http://www.politico.com/news/stories/1111/69366.html.

[8] Pub. L. 105-272, §§ 501-503, 112 Stat. 2396, 2411-12 (1998).

[9] This is codified at 50 U.S.C. § 1861.

[10] See American Library Association, Analysis of the USA Patriot Act related to Libraries, http://www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis.cfm.

[11] See American Library Council, Resolution to Continue Opposition to the Use of Section 215 of the USA Patriot Act and the Use of National Security Letters to Violate Reader Privacy (June 28, 2011) (resolving that the American Library Association "Continue[s] to oppose the use of Section 215 of the USA PATRIOT Act and the use of National Security Letters (NSL) to violate reader privacy"), available at http://connect.ala.org/node/156413; Press Release, Hon. Patrick Leahy, Leahy Renews Effort To Extend Expiring PATRIOT Act Authorities, Increase Oversight (Jan. 26, 2011), http://leahy.senate.gov/press/press_releases/release/?id=16E3E765-00E7-48EB-ADD7-A64F415E9C1D.

[12] ACLU, Reform the Patriot Act / Section 215, http://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215.

[13] 50 U.S.C. § 1861(b)(2).

[14] Letter from Ronald Weich, assistant attorney general, U.S. Dep't of Justice, to The Hon. Harry Reid, Majority Leader, U.S. Senate (April 29, 2011) (providing report pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act 1978, as amended, 50 U.S.C. § 1801 et seq., and section 118 of the USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006)), available at http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf

[15] Ellen Nakashima, FBI going to court more often to get personal Internet-usage data, Wash. Post (Oct. 25, 2011), http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html.

[16] Pub. L. 95-630, 92 Stat. 3641 (1978); 12 U.S.C. § 3414(a)(5).

[17] Pub. L. 99-569, §404, 100 Stat. 3190, 3197 (1986); 12 U.S.C. 3414(a)(5)(A) (1988).

[18] The definition of financial institutions is that found in 31 U.S.C. 5312(a)(2) and (c)(1).

[19] See Section 1114(a)(5) of the Right to Financial Privacy Act; 12 U.S.C. § 3414(a)(5).

[20] Sections 626 and 627 of the Fair Credit Reporting Act; 15 U.S.C. § 1681u.

[21] 18 U.S.C. § 2709.

[22] U.S. Dept. of Justice, Office of the Inspector General, A Review of the FBI's Use of NSLs (March 2007), at xii-xiii, available at www.usdoj.gov/oig/special/s0703b/final.pdf.

[23] Section 802 of the National Security Act; 18 U.S.C. § 2709(a).

[24] U.S. Dept. of Justice, supra note 22 at x.

[25] 15 U.SC. § 1681v

[26] ACLU, Reclaiming Patriotism: A Call to Reconsider the Patriot Act (Mar. 2009), www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf

[27] The Inspector General of the FBI, however, concluded that in earlier years (2003, 2004 and 2005), the FBI had significantly under-reported its use of NSLs when advising Congress of the frequency of their use.

[28] Eric Lichtblau & Mark Mazzetti, Military Expands Intelligence Role in U.S., New York Times (Jan. 14, 2007), http://www.nytimes.com/2007/01/14/washington/14spy.html

[29] U.S. Dept. of Justice, supra note 22 at xxvi.

[30] 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004).

[31] Id. at 476.

[32] Nakashima, supra note. 15.

[33] Id.