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 2

Law360, New York (January 30, 2012, 1:28 PM ET) -- As discussed in part 1 of this two-part article, as a practical matter, the two law enforcement tools for discovery of third-party data that were most significantly enhanced by the Patriot Act and that have given rise to significant concerns by European critics of the Patriot Act — Foreign Intelligence Surveillance Act orders and National Security Letters — should not pose a significant risk to European data on the servers of U.S.-based cloud providers. But it would be a mistake to end the analysis there.

Other Law Enforcement Tools

Search Warrants and Grand Jury Subpoenas

U.S. federal law enforcement has other, more traditional mechanisms for obtaining information it deems necessary to support its investigative efforts, such as search warrants (which must be approved by a U.S. court upon a showing of probable cause) and grand jury subpoenas, which are issued by a U.S. federal prosecutor in support of an ongoing grand jury investigation (and which a recipient may move to quash in court). These mechanisms also can be used to obtain data from the cloud. Should the risks these tools pose cause European companies to eschew U.S. cloud services?

At the outset, consider that search warrants and grand jury subpoenas are hardly new. Search warrants trace their roots in the United States back at least to the Bill of Rights (ratified in 1791), wherein the Fourth Amendment provides for protection against searches and seizures in the absence of a properly obtained warrant. Similarly, "the grand jury has been functioning as an institution for receiving evidence of criminal activity since the Magna Carta. That document guaranteed the accused the right to have a grand jury review the evidence against him prior to being charged for a criminal offense. This right, fully developed by the Seventeenth Century, was incorporated into [the U.S.] Constitution."[1]

Moreover, these mechanisms are comparable to what Europeans (and others) have in their home countries. In France, for example, the National Police and the National Gendarmerie both can execute search warrants. Article 13 of Germany's Basic Law similarly recognizes judicially ordered search warrants.[2] And, of course, U.S. search warrants have their roots in English law, where warrants continue to be a feature of modern U.K. jurisprudence. Accordingly, to the extent European consumers wish to avoid any risk that any government will access their cloud data, merely avoiding U.S. service providers is unlikely to help.

Furthermore, although the U.K. does not have the Patriot Act, it too has a law allowing the government to access, among other things, cloud data, Internet information and emails: the Regulation of Investigatory Powers Act 2000. The RIPA governs the power of U.K. authorities to carry out surveillance and investigations. It addresses when the government may intercept the content of communications, providing that such interceptions are permissible for purposes of national security, detecting or preventing serious crime, or safeguarding the economic well-being of the U.K. The RIPA also addresses when the government may obtain access to information on use of data, rather than the content itself (i.e., "envelope" information, such as the sender, receiver and time of an email message).

Under the RIPA, such envelope information can be obtained in any instance where content could be obtained, plus when needed to prevent disorder, protect public safety, protect public health or assess a tax. Use of RIPA authority is required to be both proportional and necessary to the circumstances presented. However, critics of the RIPA, much like critics of the Patriot Act, have expressed concerns that the RIPA is overbroad and that it has been misused to encroach upon basic civil liberties.[3]

MLATs

Sequestering data on European cloud servers may be an ineffective prophylactic against U.S. government access for another reason. The United States and most European governments have entered into bilateral mutual legal assistance treaties. In a typical MLAT, the two countries commit to provide one another with "the widest measure of mutual assistance in investigations or proceedings in respect of criminal offenses."[4]

Prosecutors in either country — acting through a designated central authority, e.g., the U.S. Department of Justice — can then request data, documents or testimony from the other treaty partner. In most instances, the country receiving the request agrees to provide its full cooperation, e.g., in the nation receiving the request, "[a]dministrative and judicial authorities … shall use all necessary measures available under the laws … to provide any form of assistance, not prohibited by its laws, necessary or useful for the execution of the request."[5]

Historically, MLATs did not contain any provisions expressly addressing whether the recipient of a U.S. MLAT request could deny the request on data protection grounds. Rather, most MLATs contained a general provision permitting denial of an MLAT request if executing it "would impair [the requested country's] sovereignty, security, or other essential interests or would be contrary to important public policy."[6] In 2003, the United States and the EU entered into an MLAT that specifically addresses when a U.S. MLAT request may be denied due to data protection concerns, superseding any provisions governing the denial of MLAT requests under prior bilateral MLATs between the United States and EU member states.

The U.S.-EU MLAT provides in relevant part that "[g]eneric restrictions ... for processing personal data may not be imposed ... as a condition ... to providing evidence or information."[7] The comments to the U.S.-EU MLAT explain that this provision is "meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases."[8] Accordingly, EU member states seldom deny U.S. MLAT requests, particularly those concerning terrorism investigations, for data protection reasons. Indeed, U.S. MLAT requests are largely honored by recipients throughout the world.

U.S. Jurisdictional Limitations

The discussion above addresses how various law enforcement tools under the Patriot Act operate (e.g., what information can be collected, by whom, for what purposes). But another important question is one of U.S. jurisdiction. In the United States, only a party amenable to what is known as "personal jurisdiction" can be subject to a U.S. search warrant, grand jury subpoena, NSL, FISA order, or other enforceable request for documents or data. The fundamental requirements for exercising personal jurisdiction over an individual or corporation are grounded in the U.S. Constitution, and the Patriot Act did not alter those principles (nor did it purport to do so).

The due process clause of the U.S. Constitution imposes various restraints on the exercise of judicial powers by U.S. courts. Such restraints attempt to ensure fairness in the exercise of the law. In the context of personal jurisdiction, due process considerations prohibit courts from exercising jurisdiction over a witness who lacks minimum contacts with the forum. In the case of a corporation, this means that any corporation based in the United States will be subject to U.S. jurisdiction, and thus can be subject to a FISA order, NSL, search warrant, or grand jury subpoena. The same is generally true for a non-U.S. corporation that has a branch, office or location in the United States. The same is also true for a non-U.S. corporation that conducts continuous and systematic business in the United States.

Furthermore, if an entity is subject to U.S. jurisdiction and is served with a valid subpoena, it must produce any documents within its "possession, custody, or control."[9] That means that an entity that is subject to U.S. jurisdiction must produce not just materials within the United States, but any data or materials it maintains in one of its branches or offices anywhere in the world.

The entity even may be required to produce data stored at a non-U.S. subsidiary, particularly if the subpoenaed entity can obtain non-U.S. data in the ordinary course of business. European parties can argue that, as a matter of comity, they should not be required to produce data in a manner that would violate EU data protection laws, but U.S. courts may not accept this argument[10] and (as discussed further below) in certain instances, a U.S. company's compliance with the Patriot Act is not considered a breach of EU data privacy protections.

What does this mean for non-U.S. consumers of cloud services? First, U.S. law enforcement authorities may serve a FISA order, NSL, warrant or subpoena on any cloud service provider if that company is U.S. based, or has a U.S. office, or conducts systematic or continuous U.S. business — even if the data itself is stored outside the United States. Thus, merely choosing a European cloud services provider is not enough to ensure that data is beyond the reach of U.S. jurisdiction and the Patriot Act. The European cloud services provider must have no offices in the United States, and must conduct little enough U.S. business, to ensure that it falls outside the ambit of U.S. jurisdiction.

Second, U.S. law enforcement authorities may serve a FISA order, NSL, warrant or subpoena on any cloud service customer if that company is U.S.-based, or has a U.S. branch, or conducts systematic or continuous U.S. business — even if the data itself is stored outside the United States.

Many European entities have a U.S. presence, and their U.S. presence will allow them to be subject directly to the authority of U.S. law enforcement, regardless of who they use for cloud storage. Only if both the cloud service provider and its customer avoid the United States will it be possible to avoid the direct reach of U.S. law. (As discussed above, indirect reach of U.S. law, through an MLAT request, is still possible.)

The Patriot Act and European Data Protection

The European Commission's Directive on Data Protection went into effect in October of 1998 and generally prohibits the transfer of personal data to non--European Union countries that do not meet the EU "adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. "In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a 'Safe Harbor' framework."[11]

By joining and adhering to the EU-U.S. safe harbor agreement, U.S. companies can demonstrate that their data protection practices meet the data protection adequacy requirements of the EU and the implementing legislation of the EU member states. European companies then can share data with U.S. participants in the safe harbor agreement without violating their home country data protection laws.

The safe harbor agreement contains a provision that allows U.S. companies to comply with applicable U.S. laws compelling the production of data, including the Patriot Act. It is anticipated, however, that at the World Economic Forum at the end of January 2012, the European Commission will announce a legislation to repeal the existing EU data protection directive and replace it with a more robust framework.

The new legislation might, among other things, replace EU-U.S. safe harbor regulations with a new approach that "would make it illegal for the U.S. government, for example, to invoke the Patriot Act on a company like Microsoft or Google, or any other cloud-based or data processing company, in efforts to acquire data held in the [EU]. The member states' data protection agency with authority over the company's European headquarters would have to agree to the data transfer."[12]

The foregoing developments may significantly affect the legal landscape for protection of data in the cloud servers in the cross-border context, and thus should be monitored closely. However, it may be years before the new legislation is enacted (the current EU Data Protection Directive took three years). By that time, changes in technology may present entirely new challenges and considerations

Conclusion

Consumers of cloud services are wise to consider all types of risk to their data, whether from their home country government or another country's government. Merely avoiding U.S. cloud service providers based on concerns about the Patriot Act does not solve the problem. That choice alone provides no assurance that cloud data is beyond the reach of the Patriot Act and provides no protection against the risk that non-U.S. governments will access the cloud-stored data, either on their own initiative or in response to an MLAT request from the United States.

Rather than making a decision based solely on the home country of competing cloud providers, informed consumers of cloud services should (1) consult legal counsel in their home country, in any jurisdiction where their data may be stored, and in any jurisdiction where their cloud service provider does business, (2) closely review their cloud services contracts and ask their providers questions, and (3) carefully consider all the relevant risks before making a decision.

--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.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Grand Jury Proceedings (Williams) v. U.S., 995 F.2d 1013, 1016 n.6 (11th Cir. 1993).

[2] Dominik Hanf, Constitutional Court Reaffirms Privacy of the Home in Search and Seizure Decision, German L. J., http://www.germanlawjournal.com/article.php?id=57.

[3] Big Brother Watch, One Year On: The Coalition and Civil Liberties (May 2011), http://bigbrotherwatch.typepad.com/home/research.html/; Gordon Rayner & Richard Alleyne, Council spy cases hit 1,000 a month, Telegraph (Apr. 12, 2008, 12:01 AM BST), http://www.telegraph.co.uk/news/uknews/1584808/Council-spy-cases-hit-1000-a-month.html.

[4] See MLAT, U.S.-Fr., art. 1, Dec. 10, 1998, S. Treaty Doc. 106-17, available at untreaty.un.org/unts/144078_158780/16/2/7131.pdf; MLAT, U.S.-Ger., art. 1, Oct. 14, 2003, S. Treaty Doc. 108-27 (same), available at http://purl.access.gpo.gov/GPO/LPS57313.

[5] MLAT, U.S.-Fr., at art. 8.; MLAT, U.S.-Ger., at art. 10 ("If necessary, compulsory measures shall be applied to execute a request for taking testimony or producing documents … in the same manner as in criminal investigations or proceedings in the Requested State."); MLAT, U.S.-U.K., art. 8, Jan. 6, 1994, S. Treaty Doc. 104-2, available at, http://tinyurl.com/cqvtxhl ("A person in the territory of the Requested Party from whom evidence is requested pursuant to this Treaty may be compelled, if necessary, to appear in order to testify or produce documents, records, or articles of evidence by subpoena or such other method as may be permitted under the law of the Requested Party.").

[6] MLAT, U.S.-U.K.,, at art. 3, ¶ 1(a); MLAT, U.S.-Ger. , at art. 3 (same); MLAT, U.S.-Fr., at art. 6, ¶ 1(b) (same).

[7] MLAT, U.S.-EU, art. 9, ¶ 2(b), June 25, 2003, S. Treaty Doc. 109-13, available at http://tinyurl.com/7d6qhs7.

[8] See MLAT, U.S.-EU, at Explanatory Note on art. 9.

[9] See In re Grand Jury Subpoena, 646 F.2d 963 (5th Cir. 1981); 5A Moore's Federal Practice p 45.05(1) (2d ed. 1980); U.S. v. King, 1997 (S.D.N.Y. Sept. 19, 1997)

[10] See AccessData Corp. v. Alste Techn. Gmbh, 2010 (D. Utah Jan. 21, 2010).

[11] http://export.gov/safeharbor/.

[12] Zack Whittaker, European data protection law proposals revealed, ZDNet (Dec. 7, 2011, 4:02 PM PST), http://www.zdnet.com/blog/london/european-data-protection-law-proposals-revealed/1365.