Disclosure of Customer Data under the US Patriot ACT and the relevant Greek Legislation – a brief memo

Contents

1. THE PATRIOT ACT

The **USA Patriot Act** ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001") mainly expanded the following discovery and enforcement mechanisms already available under US law, i.e. (a) **FISA Orders** and (b) **National Security Letters**, the impact of which will be further discussed:

(a) FISA Orders

According to the U.S. legal framework prior to the Patriot Act ("Foreign Intelligence Surveillance Act"), the FBI could apply to the Foreign Intelligence Surveillance Courts

(FISC) for a FISA Order to obtain "*access to certain business records for foreign intelligence and international terrorism investigations*". The scope of such orders was originally limited. Title II of the Patriot Act (SEC. 501 - "Enhanced Surveillance Procedures"), expanded the reach of FISA Orders to allow the FBI to obtain *"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*** *and clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*[1]" (emphasis added). **Such provision is interpreted in a way to include data in the cloud**.

From a practical perspective, it should be noted that the FBI rarely uses FISA orders. According to the 2011 Foreign Intelligence Surveillance Act (FISA) Report, in 2011, the US Government made only 205 applications to the FISC for access to certain business records for foreign intelligence purposes.

(b) **National Security Letters (NSL)**

NSLs are a form of administrative subpoena issued to an entity or organization to disclose certain records and data pertaining to individuals. NSLs are issued by U.S. Government Agencies, mainly the FBI, and need not receive prior approval of a judge. The NSL mechanism existed well before the enactment of the Patriot Act, but the Patriot Act expanded its scope, however, always relevant to international terrorism or clandestine intelligence activities. Even under such expanded scope, the data that can be disclosed to U.S. Authorities by internet service providers are limited to "*customer name, address, length of service and local and long distance toll billing records"* (non-content information). The recipient of a NSL request may petition a U.S. District Court for an Order modifying or setting aside the request. The Federal Court may modify or quash the NSL request if compliance would be unreasonable, oppressive, or otherwise unlawful[2].

[1] The right to freedom of religion and freedom of expression from government interference ("*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances*").
[2] CRS Report for Congress, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*, http://www.fas.org/sgp/crs/intel/RL33332.pdf

From a practical perspective and according to the 2011 Foreign Intelligence Surveillance Act (FISA) Report, in 2011, the FBI made 16,511 National Security Letter requests for information pertaining to 7,201 different U.S. persons. This is a substantial **decrease** from the 24,287 national security letter requests concerning 14,212 U.S. persons in 2010.

Further to the above enforcement mechanisms, other legal tools available to U.S. law enforcement agencies include **search warrants** (which require prior approval by a U.S. court upon a showing of probable cause) and **grand jury subpoenas** (issued by a U.S. federal prosecutor in support of an ongoing grand jury investigation and in order to gather evidence to make the case and which a recipient may move to quash in court), and disclosure requests made on the basis of **Mutual Legal Assistance Treaties (MLAT),** which allow generally for the exchange of admissible evidence and information in criminal matters. A MLAT is in force between the U.S. and the E.U. since 2003. The MLAT between the U.S. and the E.U. applies in relation to MLATs between the E.U. Member States and the U.S. in force[3]. Greece and the U.S. have signed a MLAT[4], which is in force since November 20th, 2001 and its scope covers the assistance in connection with the investigation, prosecution and prevention of offenses and in proceedings related to criminal matters (including organized crime, murder, etc.). Such assistance includes (a) providing documents and records; (b) locating or identifying persons or items; (c) executing searches and seizures.

Again, search warrants, grand jury subpoenas and MLATs can be used in order to obtain data stored in the cloud.

2. CAN THE PATRIOT ACT 'REACH' NON-U.S. ENTITIES?

Corporations with a corporate seat in the U.S. will certainly be subject to U.S. jurisdiction. It is possible that subject to U.S. jurisdiction will also be **non-U.S. entities** with a form/type of corporate 'presence' in the U.S. (e.g. if such entity has a U.S. Brach Office, **or even if it**

[3] http://acfcs.org/sites/default/files/United%20States%20Mutual%20Legal%20Assistance%20Treaties.pdf
[4] http://www.state.gov/documents/organization/122864.pdf

conducts "*continuous and systematic*"[5] business in the U.S.). Similarly, the Patriot Act could apply to an E.U. based entity using the services of a U.S. subsidiary or even of a third party for data processing (e.g. for the provision of hosting services).

When an entity subject to U.S. jurisdiction is served e.g. with a valid FISA Order, such entity could be expected to disclose even data stored abroad, at a non-US subsidiary or Group entity.

Further, many European businesses have a U.S. presence in the sense described above, and such U.S. presence could make the businesses in question directly subject to the authority of U.S. law enforcement, regardless of the location of the company they use for cloud storage.

Thus, merely choosing an E.U. based cloud service provider is not enough to ensure that customer data is beyond the reach of U.S. jurisdiction and the Patriot Act.

3. THE GREEK LAW

The Greek Constitution (article 9) establishes the "*absolute inviolability*" of secrecy of communications, which can be side-stepped only for very specific cases (national security and a very limited number of felonies) and only under the guarantees and supervision of the judiciary and the involvement of a constitutionally established independent authority (with the sole purpose of safeguarding the confidentiality and secrecy of communications).

A list of the felonies for which 'lifting of secrecy of communications' can be ordered and the procedures, time limits and technical and organizational safeguards that need to be followed are analyzed in Law 2225/1994 and PD 47/2005[6]. Only the competent Public Prosecutor or a judicial authority or other political, military or police public authority,

[5] *Inter alia*: *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 2011 WL 2518815; *Perkins v. Benguet Consolidated Mining Co.*, 342 U.S. 437 (1952)

[6] Articles 248-250 of the Greek Penal Code lay down sanctions for the violation of secrecy by post officials and employees of telecommunication companies and articles 370 and 370A of the Greek Penal Code law down sanctions for the violation of secrecy of letters and telephone calls and private communications.

competent for an issue of national security requiring the 'lifting of secrecy', may submit a request for 'lifting of secrecy', which then can be ordered by the Appeals Prosecutor or the competent Judicial Council (exceptionally by the Public Prosecutor).

The Hellenic Authority for Communication Security and Privacy (ADAE) reviews such judicial Orders and monitors compliance with the conditions and the procedures of the 'lifting of secrecy'.

The 'lifting of secrecy' applies only to communication conducted via communication networks or via communication service providers. The **types and forms of communication** which are subject to the lifting of secrecy are, *inter alia*, telephone (fixed and mobile), data communication via data networks, internet communication, wireless communication, satellite communication, and services provided in the framework of the above types/forms (e.g. automatic answering machine, SMS/MMS, access to websites, access to databases, e-mail, electronic transactions, directory information, emergency services). **Therefore, it is clear that data stored in the cloud are certainly within the scope of the 'lifting of secrecy' provisions.**

However, similar to the US Patriot Act, the above provisions apply only to specific criminal cases, i.e. **(a)** to national security cases, and **(b)** to a limited number of felonies, which include *inter alia* treason, espionage, organized crime, forgery, bribery, murder, robbery, and extortion.

From a practical perspective and according to the 2011 Hellenic Authority for Communication Security and Privacy Annual Report, ADAE, in 2011, received and reviewed 3,472 Prosecutor Orders regarding 'lifting of secrecy' for national security issues (a significant increase from the 2,281 in 2010), 4,061 Requests for extension of previously issued Prosecutor Orders (a significant increase from the 2,965 in 2010), and 1,743 Judicial Council Orders regarding 'lifting of secrecy' for serious felonies (a significant increase from the 1,169 in 2010).

The current legal and political debate[7] in Greece on the necessity of lowering the requirements set by the current legislation is indicative of the hurdles the current framework poses to law enforcement agencies. Such debate includes a discussion on whether the protection of confidentiality covers only the content of the communication or traffic data as well and, in this scope, if the procedure for the 'lifting of secrecy' applies to traffic data, in which case an Order by the Appeals Prosecutor or the competent Judicial Council is required, or simply a Public Prosecutor's Order is sufficient for the disclosure of such data.

Lawful interception/wiretapping of electronic data is under specific circumstances a legal activity under Greek law, which predated the U.S. Patriot Act and which is available under both jurisdictions and, in this context, the U.S. Patriot Act does not introduce an altogether new 'threat' for cloud computing services for Greek businesses/customers.

4. CONCLUSIONS

Based on the above, it is obvious that the mere fact that a Greek business/customer avoids U.S. based cloud service providers **(a)** does not exclude the possibility of exposure to U.S. jurisdiction and of customer data being disclosed or intercepted pursuant to U.S. law (incl. the Patriot Act), and most importantly **(b)** it provides no assurance that customer data will not be disclosed by an E.U. based cloud service provider to the U.S. enforcement agencies pursuant to a valid MLAT request, whereas **(c)** in all cases Greek Constitution and Greek security and privacy legislation (which include provisions for the 'lifting of confidentiality' and interception/wiretapping of electronic data) will apply to cloud providers based in Greece. It is further noted that in both legal systems (the U.S. and Greek), the enforcement of such interception and disclosure measures is limited to specific, very serious crimes and felonies (incl. terrorism and organized crime).

[7] See *inter alia*: 9/2009 Opinion of Public Prosecutor of the Greek Supreme Court (in Greek); 9/2011 Opinion of Public Prosecutor of the Greek Supreme Court (in Greek); 1/2005 Opinion of the Hellenic Authority for Communication Security and Privacy (in Greek)

Referring to a recent academic paper on cloud contracts and quoting Hon, Millard and Walden[8], *the United States is not the only nation that may access data for anti-terrorism or anti-crime purposes and, the current high profile of [the Patriot] Act may perhaps reflect some marketing opportunism and certain political concerns regarding the United States exercising its powers extra-territorially, more than legal differences.*

[8] Hon, W. Kuan, Millard, Christopher and Walden, Ian, *Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now* (May 9, 2012). 16 STAN. TECH. L. REV. 81 (2012); Queen Mary School of Law Legal Studies Research Paper No. 117/2012. Available at SSRN: http://ssrn.com/abstract=2055199 or http://dx.doi.org/10.2139/ssrn.2055199