Linklaters

October 2011

Law Enforcement and Cloud Computing

Cloud computing is gaining momentum as the new IT paradigm and a leading business and economic model. In weighing the pros and cons of going cloud, users must assess what this means for them in terms of security and data protection, just how safe, private and confidential their data is in the cloud, both from a technical and legal point of view. In this regard, the ubiquitous and transnational nature of cloud computing raises considerable questions on applicable law and competent jurisdiction.

From an EU perspective, Dutch Liberal MEP Sophie in 't Veld has voiced her concern about the reach of the so-called USA PATRIOT Act in the European realm. Within the EU, the USA PATRIOT Act is often perceived as a sort of broad blanket license for law enforcement agencies to oblige individuals and companies to disclose certain records or information they hold and which are believed to be relevant for counterterrorism or counter-intelligence investigations.

One of the most controversial provisions of the USA PATRIOT Act is Section 215, which amends the Foreign Intelligence Surveillance Act of 1978 to permit the FBI to obtain an order ("**Section 215 Orders**") from the Foreign Intelligence Surveillance Court demanding "*any tangible thing (including books, records, papers, documents and other items)*" believed to be relevant to an authorised investigation regarding international terrorism or espionage[1]. The USA PATRIOT Act also expanded the use of National Security Letters ("**NSLs**"). NSLs permit the FBI and other law enforcement agencies to obtain information within certain prescribed categories: financial records, telephone and e-mail communications data and Internet searches. NSLs may be issued where the records sought are relevant to an authorised counterterrorism or counter-intelligence investigation.

This is worrisome according to Mrs. in 't Veld as it would enable US authorities to access personal data stored in the EU by companies with headquarters in the US based on US legislation, while disregarding EU legislation on data protection.

[1] 50 U.S.C. § 1861(a)(1)

Ultimately, the concerns expressed are usually based on the assumption that European legislation is fundamentally more protective than the US'. However, the current debate on the compatibility of the USA PATRIOT Act with EU data protection laws and on the alleged "*vulnerability*" of data placed in a US cloud environment appears to be based upon a misapprehension of the EU Data Protection Directive[2] and the broader legal framework within the EU.

The EU's centrepiece legislation on data protection explicitly enables Member States to make away with privacy protections, which would otherwise apply, for a series of reasons, among which "*public security*", "*State security (including the economic well-being of the State, when the processing operation relates to State security matters)*" and "*the activities of the State in areas of criminal law*"[3]. Many EU Member States have provided for specific exemptions in their national data protection laws, resulting in either the national data protection law not being applicable to these kinds of activities at all or certain protections provided for by the national data protection law not being applicable to these kind of activities. Counterterrorism and counter-intelligence investigations carried out by law enforcement agencies thus benefit from an exemption from the national data protection law in most EU Member States.

Law enforcement agencies within the EU operate by virtue of the specific powers they are granted to gather information and evidence and many EU Member States possess legislation which grants extensive and often intrusive investigatory powers to national authorities.

In the immediate aftermath of the 9/11 terrorist attacks, France adopted the Act No 2001-1062 of 15 November 2001 on day-to-day security[4], significantly strengthening the powers of French law enforcement agencies.

Under the French Code of Criminal Procedure[5], French law enforcement agencies[6] can order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress (including those produced from a registered computer or data processing system) to provide them with these documents. These provisions are quite broad: as long as they are relevant to an inquiry in process, the authorities may require any document from any person. The documents so requested may relate to a person other than the one being subject to the disclosure order (e.g. a cloud provider). Specific provisions have implemented such proceedings in the digital environment. The French Code of Criminal Procedure[7] authorises law enforcement agencies, intervening by means of telecommunications or computers, to request any public organisations or private legal persons, with the exception of associations or non profit religious, philosophical, political or trade union members and professional journalists, to communicate information helpful for

[2] Directive 95/46/EC on the protection of individuals with respect to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995, p.0031-0050.
[3] Article 3.2 of the EU Data Protection Directive.
[4] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[5] Articles 60-1, 77-1-1 and 99-3 of the French Code of Criminal Procedure.
[6] E.g., a public prosecutor, a judicial police officer or an investigating judge.
[7] Articles 60-2, 77-1-2 and 99-4 of the French Code of Criminal Procedure.

the discovery of the truth in an ongoing investigation (except when the secrecy is protected by statute) where it is stored in one or more computer or data processing systems that they administer.

The recent French Act No 2011-267 of 14 March 2011 in relation to domestic security matters allows an investigating judge to authorise, for offences committed by an organised group, judicial police officers and agents to set up technical devices allowing them to access, record and transmit electronic data, *without the consent of the person being subject to this measure*, as they appear on the screen for the user of the computer or as they are being entered on a keyboard. Although the authorised operations are somewhat limited as the authorities cannot search within a computer system and can only monitor it as it is being used, it remains quite intrusive since data are being captured *without the user's knowledge*.

Likewise, the French Code of Post and Electronic Communications[8] requires telecom operators and internet providers to store technical data regarding electronic communications of their customers. Since the Act No 2006-64 of 23 January 2006 related to the fight against terrorism, Article 34-1 of the French Code of Post and Electronic Communications has been modified to impose the same retention obligation to persons who provide, as a principal or accessory professional activity, an access to an online communication via a network, even free of charge. Furthermore, Article 6 II of the French Act No 2004-575 of 21 June 2004 in relation to confidence in digital economy obliges public electronic communication service providers and providers of hosting services of publicly accessible content to retain data allowing the identification of anyone having contributed to the creation of the content or of part of the content of the services they provide. In addition to the prerogatives of the judicial authorities, Article 6 of the French Act No 2006-64 inserted Article 34-1-1 in the Code and modified Article 6 II of the Act No 2004-575 in order to authorise, for the purpose of preventing acts of terrorism, agents individually designated and duly empowered from the police services to request communication of any of the aforementioned data retained by the aforementioned operators.

In Spain, the Act No 12/2003 of 21 March 2003 regarding the prevention and blocking of terrorism financing has granted the *Comisión de Vigilancia de Actividades de Financiación del Terrorismo*[9] (CVAFT) broad powers to request information from and has imposed an obligation to cooperate upon all persons and organisations subject to the Spanish anti-money laundering laws. In addition, the CVAFT has access to information held by tax administration, social security administration, the Bank of Spain, the stock exchange market regulator and the insurance regulator. Persons and organisations subject to Spanish anti-money laundering laws have broad obligations to provide information and are prohibited to report to the persons concerned by such information that they have been reported. Also in Spain, under the Act No 25/2007 on the retention of data of electronic communications and networks, electronic communications providers have

[8] Article 34-1 of the French Code of Post and Electronic Communications.
[9] Commission for Vigilance of Activities relating to the Financing of Terrorism.

broad obligations in relation to retention and disclosure of data regarding electronic communications.

It is inherent to any criminal, counterterrorism or counter-intelligence investigation that the investigation by law enforcement agencies is secret and that, as a result, third parties from whom information or records are sought are prohibited from disclosing that law enforcement authorities sought and/or obtained information from them. Unsurprisingly, Section 215 Orders and NSLs issued under the USA PATRIOT Act are most often accompanied by a compulsory non-disclosure or "gag" order. Again, this is however not a prerogative of US law. In most EU Member States, criminal investigations are protected by the fundamental principle of secrecy. In addition, the law of EU Member States also frequently provides for non-disclosure obligations imposed upon third parties from whom information is sought. For example, the Belgian Code of Criminal Procedure[10] imposes an obligation on electronic communications services providers to cooperate with the public prosecutor and disclose certain information relating to the identity of users in the pursuit of criminal investigations. Whoever, in the course of his function, has knowledge of such a request is bound to secrecy. A violation of said non-disclosure obligation is criminally sanctioned. This example shows that, in the EU too, cloud providers may in certain cases be compelled to hand over certain information to law enforcement authorities without the data owner or data subject being specifically informed of such disclosure[11].

Another aspect of the USA PATRIOT Act that has received attention in the EU debate on cloud computing is the fact that Section 215 Orders and NSLs issued under the USA PATRIOT Act are often accompanied by *subpoenas*, i.e. amounts payable by the person to which the order or letter is addressed in the event of non-compliance. Although the concept of a *subpoena* as such is unknown in many EU jurisdictions, many EU Member States have similar means in place to ensure cooperation with law enforcement authorities. For instance, in Belgium, failure by an electronic communications services provider to cooperate with the public prosecutor and disclose certain information relating to the identity of users in the pursuit of criminal investigations is criminally sanctioned with fines up to EUR 55,000[12].

Concerns have also been voiced in connection with the power of law enforcement agencies under the USA PATRIOT Act to seek information *directly* from so-called "third parties" (such as cloud providers) having a US presence, thus avoiding the need to rely upon established mechanisms or arrangements for international cooperation in criminal matters such as e.g. the Cybercrime Convention (which itself recognises the validity of direct trans-border access with the lawful and voluntary consent of the person having

[10] Article 46bis of the Belgian Code of Criminal Procedure.

[11] Consequently, from a compliance point of view, cloud providers, US and EU alike, would be well-advised to ensure that their privacy policies and/or general terms and conditions foresee that they may be obliged to disclose certain data to law enforcement agencies when so requested in accordance with applicable law.

[12] Article 46bis, *§ 2 in fine* of the Belgian Code of Criminal Procedure. See, for an application, the *Yahoo!* case referred to *infra*.

lawful authority to disclose the data[13]). However, issues of international jurisdiction in relation to the internet are not specific to US law, let alone the USA PATRIOT Act. Most EU Member States face similar issues with the application of their national laws in the internet environment. In 2009, the US based company *Yahoo!* was imposed a fine by a Belgian Criminal Court for failing to identify the users of a number of webmail accounts to the Belgian public prosecutor. While *Yahoo!* had argued that the United States and Belgium had a formal international treaty which the prosecutor should follow to properly seek information from a US company like *Yahoo!*, instead of trying to obtain it directly from *Yahoo!*, the court considered that *Yahoo!* was an electronic communication services provider (ESP) within the meaning of the Belgian Code of Criminal Procedure and that the obligation to cooperate with the public prosecutor applied to all ESPs which operate or are found to operate on Belgian territory, regardless of whether or not they are actually established in Belgium. This judgment was overturned by the Court of Appeal of Ghent in 2010. The Court considered that the Code of Criminal Procedure was to be read in the light of the law on Electronic Communications of 13 June 2005 that defines an ESP as a company offering services consisting in the transmission (including switching operations and routing) of signals on electronic communication networks and that *Yahoo!* was thus not to be regarded as an ESP since its webmail relied on the Internet to send out emails. In January 2011 however, the Belgian Supreme Court reversed the Court of Appeal's decision ruling that, according to the principle of autonomy of criminal law, the concept of electronic communications services provider in the Belgian Code of Criminal Procedure bore an autonomous meaning from that of the law on Electronic Communications. The case illustrates that the jurisdiction issues that privacy-activists now put forward with respect to the USA PATRIOT Act may also be a concern with respect to EU Member States' (criminal or other) laws.

The above examples show that both in the US and in the EU cloud providers may be obliged to cooperate with law enforcement agencies, resulting in the disclosure of (personal) data without the data owner or the data subject being made aware thereof. Non-compliance by cloud providers with requests for information by law enforcement agencies is, both in the US and in the EU, often sanctioned with *subpoenas* (US) or equivalent criminal sanctions (EU). Moreover, the issue of extra-territorial application of national laws in an internet environment is an issue that has been prevalent in the debate on the legal aspects of the internet since its inception.

From a cloud user's perspective, the above review essentially means that cloud users should apply sound information management practices considering the appropriate classification of data – whether personal data or not – based on the risk of disclosure and local legislation's requirements. Those considerations should then be used to match the security and isolation requirements of the various categories of data with the security of the storage site. Sound information management practice, not the USA PATRIOT Act or

[13] Article 32 b. of the Cybercrime Convention; See also I. Walden, "Law Enforcement Access in a Cloud Environment", Queen Mary University of London, School of Law, Legal Studies Research Paper No. 74/2011, available at http://ssrn.com/abstract=1781067.

similar laws in other countries, should govern decisions regarding what data is appropriate for what range of storage sites, including use of cloud services. In the end, law enforcement access to data is not a new issue nor an issue that is specific to cloud computing. It also arises in the context of e.g. outsourcing and off shoring, IT service delivery models which already exist for more than two decades.[14]

Tanguy Van Overstraeten
Partner
Linklaters LLP

Bastiaan Bruyndonckx
Counsel
Linklaters LLP

Rue Brederode 13

B - 1000 Brussels

Telephone (+32) 2 501 94 11
Facsimile (+32) 2 501 94 94

Linklaters.com

[14] This article has been written with the input of Linklaters LLP's Paris and Madrid offices in respect of French resp. Spanish law.