Openforum Academy

Can we determine and restrict the location of our data in the Cloud, and when do we need to?

Report

ROUND TABLE: Can we determine and restrict the location of our data in the Cloud, and when do we need to?

22 May 2013, Silken Berlaymont Hotel, Brussels

Disclaimer

This report is prepared by the rapporteur, Dr. E. Altsitsiadis, for OpenForum Academy (OFA). The summaries of the speaker presentations and panel discussions in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion. The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

Speakers

Christopher Wolf - *Director of Hogan Lovells' Privacy and Information Management practice group*

Winston Maxwell - *Partner Hogan Lovells Paris*

Jan Ostoja-Ostaszewski - *Directorate General for Justice, European Commission*

Moderator: Graham Taylor, CEO of OpenForum Europe.

Rapporteur: Dr. Efthymios Altsitsiadis, Senior Researcher KU Leuven - Research Centre for Marketing and Consumer Science

Foreword

Last year OpenForum Academy hosted a Round Table discussion on “Who do you Trust with your Data in the Cloud?” which featured the launch of a report by Hogan Lovells on Government Access to Data in the Cloud and a comparison of the Patriot Act with national schemes across Europe. That report has been widely quoted since, with some praising it for shedding light on the situation and others challenging its conclusions. Since then the thinking on the impact of Cloud Computing across Europe has developed significantly, the European Commission has published its Communication, yet the same key question remains - **Can we determine and restrict the location of our data in the Cloud, and when do we need to?**

In an updated session we have invited back Hogan Lovells to respond to the questions previously raised, the challenges to their conclusions, and to present an update to the Report which specifically now includes the impact of the US authorities Foreign Intelligence Surveillance Act Amendment (FISAA). So is it all just a matter of players jostling for market positions and using such arguments to promote their business interests or does Europe have to focus on this issue, particularly in light of the upcoming TTIP negotiations and finalization of the proposed European regulation on data protection? Do we need additional legislation or are we able to operate in a way that balances national security needs with the data protection needs of the citizen and users?

Christopher Wolf and Winston Maxwell – respectively, Director of the Privacy and Information Management Practice Group, and Partner in Paris for Hogan Lovells, presented their updated report; this was then responded to by Jan Ostoja-Ostaszewski from DG Justice of the Commission, and other participants from the academia, civil society and industry. The report that follows reflects the lively debate that transpired.

Introduction

Mr. Graham Taylor kicked off the round table by stressing the mission of OpenForum Europe for an open competitive IT market and its dedication and campaigning against lock-in in all of its facets throughout the ICT field. Mr. Taylor introduced the OpenForum Academy, a think tank of expert fellows set to bridge academia and industry in order to spring fresh ideas in favor of openness in IT market.

The dramatic growth in the uptake of cloud computing was followed with the outbreak of issues surrounding the cloud; cyber-security, trust, protection and portability of data to name a few. How much are we talking about a global market and how much can Europe do in that global market to maximize the opportunities for innovation in favor of European SMEs and citizens? A series of fundamental questions have emerged relating to how you manage the data; what happens to the data; who owns your data? The continuing question towards the European Commission is at what point do you act as a facilitator and at what point as a legislator?

Mr. Taylor linked the current discussion to the last year's OFA round table about the Patriot Act and the presentation of the Hogan Lovells paper that removed many of the misconceptions surrounding it and prompted that there are not many differences among US and EU governments in this respect. As the controversy since last year increased, Hogan Lovells will present an update of that paper and clarify what exactly it is they are talking about and what the impact for Europe is.

Christopher Wolf briefly talked about his role as founder of Future Privacy Forum and stressed one of the hallmarks of the Hogan Lovells privacy and data protection practice is not to only represent customers but to contribute to the privacy public policy dialogue. Last year they addressed what they believe was a skewed discussion on the US Patriot Act with regard to access of cloud data by law enforcement. They presented in their paper a variety of laws from around the world that were similar in effect if not exactly the same in content as the Patriot Act. Recently, after the Patriot Act discussion, some have focused their attention on Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), enacted under the FISA Amendments Act of 2008 ("FAA"). Quoting MEP Sophia in t' Veld's recent statement (that FISA allows the US authorities to browse the cloud without a warrant), he stressed that today's discussion should be able to clarify the misperception embodied in that statement.

Mr. Wolf clarified that this work was part of the activities of a group within their firm that does scholarly work regularly and further stressed that this work was not for a governmental client.

Winston Maxwell provided the context of FISA since its enactment and noted the similarities in process with France. He noted that one of the reasons for the FISA amendment on 2008 was that the intelligence community felt that FISA requirement of specific targets for warrants precluded broader investigations of terrorism.

Mr. Wolf explained the judicial approvals required for national security surveillance under FISA as well as the legislative review required. He explained that as with the Patriot Act, section 1881a has been used to (incorrectly) argue that the US government has greater access to data in the cloud than other governments.

Mr. Maxwell highlighted the commercial aspects of the argument; European cloud providers claim that one should feel more comfortable using their services rather their US competitors. The debate on these FISA aspects requires a side by side analysis with national defense and espionage provisions of other countries (e.g. France, Great Britain, Germany). In most cases of developed countries there are two main chapters; the code of criminal procedure and the code of internal security (their own version of FISA) where usually a court is not involved in that second silo. There are also other protections required by the European court of justice but these are not judicial necessarily.

Mr. Wolf noted that their white paper tries to address the criticisms of Section 1881a and tried to compare the nature and extent of government access to data in the cloud for terrorism and counterintelligence purposes in many jurisdictions around the world. The request for surveillance are subject to prior authorization by the foreign intelligence surveillance court (FISC) except in extraordinary circumstances and even then the court needs to be informed of the surveillance and needs to approve it; Section 1881a does not give the US government a carte blanche to seize whatever information they wish from cloud providers. The paper sets forth the limitations on the government surveillance authority: the requirement that it be conducted only to obtain foreign intelligence information, that there will be judicial and legislative oversight, and comparable transparency to that of other countries.

Mr. Maxwell stressed that one of the key safeguards under FISA is that it is available only to obtain foreign intelligence information, which is limited to information about an agent of a foreign government or a terrorist organization and in either case there has to be a linkage to a foreign agent. Private business records, academic data or political opinions do not constitute foreign intelligence information and the court and the Congress enforces that very specific definition. The Congress recently signaled its intent to exempt the private political views of non-US citizens from the scope of what will be collected and it views the activities of FISC through that prism.

Mr. Maxwell talked about the situation in France and the commonalities and pronounced his upcoming paper on the French framework while Mr. Wolf added that there are concerns for the UK regime as well. What is important though is to compare things that are indeed comparable. The concerns and the decision of what level of risk he is going to assume is up to every cloud customer but that decision should be based on facts and the law and not be up to assumptions.

Jan Ostoja-Ostaszewski highlighted the importance of trust and innovation on cloud. Cloud must be developed and we need to support innovation. The EC is in the middle of reforming its data protection system in the EU with two legislative proposals set to strengthen the rights of data subjects and facilitate international transfers. With regard to security issues he referred to a problem of jurisdiction. It is important to make sure that when the access to personal data is provided to third countries it is being done in a way which is in line with our laws; in the context of EU-US relations such access has to be founded on the existing legal instruments such as Mutual Legal Assistance.

Access by national security or agencies fighting terrorism and criminal acts should be further discussed in the context of transatlantic relations. The principles of personal data protection are being discussed with the US; we need to agree on several common principles, their implementation, and the rights of citizens when their data is accessed for law enforcement purposes. In the near future other players (non EU or US) might enter the cloud arena and the discussion would be much more challenging. Therefore it is important to find an EU-US agreement and a common position in order to be able to defend this position in this near future.

Discussion

Disclaimer: These comments were taken from the general part of the meeting and do not necessarily represent any of the speakers' views or those of their organisations. The discussion took place under Chatham House Rule and therefore names and affiliations of participants are not reported.

- **Question:** FISA is marked for having a specific extraterritorial provision. Are other countries putting into place similar kinds of extraterritorial provisions, or not?

The French law (internal security code, 1991) does not have any provision in that code that targets interceptions outside France. There is anecdotal evidence in the media about the sophistication of the French intelligence forces. Those surveillances outside France don't come out of any judicial framework. The security interceptions involve necessarily service providers operating in France; there has to be a physical connection to France in order to intercept communications.

- **Question:** It seems that we are just following the national security programmes. Is that something that we should base all the EU cloud strategy on, in terms of data privacy, solvency and so on?

What we want to avoid is the situation where a cloud service provider is put into a legal bind because they are complying with the request for data access to a US law enforcement agency with a court order preventing provisioning of this information.

There are provisions in the FISA which could prevent declaration that the investigation is under way because of concerns about prejudicion to the investigation.

This is one of the reasons the mutual legal assistance discussion is so important, because unless there is a solution in how to handle this, we have a situation where cloud providers are possibly be put in a position of legal jeopardy.

There should be efforts to harmonize the conflicts that arise. The same concerns, however, are applicable to European Cloud providers faced with an order to provide information about US citizens.

- **Question:** Is the harmonization discussion part of the EU-US discussion?

The principles and ways of dealing with personal data in the context of law conflicts are there. For the EU it is clear that we have our law and cloud

providers must comply with our law. If there is a request from our jurisdiction they might indeed be in the breach of law.

Comment: The central fallacy is that we are asked to agree that because the US has excellent safeguards for US citizens in the US, while in certain cases EU countries have inferior safeguards for their own citizens that we should be happy with the conflicting situation.

Cloud software infrastructure is typically controlled during US day time from Seattle or San Antonio or sometimes the East Coast and typically the night time from Singapore or India. On the US jurisdiction information can be sucked out of the cloud in a state of continuous mass surveillance. 1881a undoubtedly discriminates against non US persons; firstly it is only about acquiring foreign intelligence information about non-US citizens located outside the US, secondly it is much more severe if you are not an US person.

Is it a warrant or not? The authorization by the director of national intelligence is a blanket categorical authorization; it practically allows the DTI box to scan data about certain subjects of interest to US foreign policy, it does not have to name targets and has no categorical necessity other than filtering out data with respect to US persons.

In response it was suggested that there has to be co-authorization and there is legislative oversight; the FISA does not give the US intelligence authorities the ability to browse the cloud.

The congress is charged with ensuring that the surveillance is done with the principle of data minimization.

A comment was raised about how this principle is implemented and that there are techniques employed by the law enforcement agencies that do much more than mass surveillance.

Definition of foreign intelligence information: Quote from the statute: **"**Information that relates to the ability of the US to protect against actual or potential attacks or other grave hostile acts of a foreign power or agent of a foreign power…"

The definition does not permit one to pick up private political organizations or opinions. The authority, the legislative history and the testimony when they renewed the FISA indicate that foreign intelligence information category is fairly restricted; we cannot get into all the details though because they are classified.

- **Question:** From what has been said so far, it can be argued that the level of protection for a citizen in the US is higher than in EU (e.g. in France). Does the EU intend to address this imbalance?

A comment to the question added that the protection is better in the US if you are a US citizen.

A cynical look would suggest that governments will have the ability to potentially manipulate words in a law; companies are the ones who get caught in the middle. It is in the economic interest of the US and EU (and China being the next frontier) to get these imbalances sorted out and stable in some kind of trust framework that works.

- **Question:** With regard to democratic oversight mechanisms, is there a scale in the study for different countries (e.g. from highest level of comfort to the least)?

The key safeguard is that there is a specific law that contemplates this sort of intrusion into privacy and there has to be safeguards necessary for a democratic society.

In France there is first a control by an independent high level member of the executive; the person who asks for the permission has to be different than the person who grants it.

A number of countries have concluded that they cannot use normal judges. The US decided to use federal judges. Under FISA you have FISA court; a court made up of normal federal judges who do not come from the military or the CIA, they are civil judges appointed for life.

Comment: All of this is called comfort if you are not an US person. The basic asymmetry with the European Convention rights which apply equally irrespective of nationality is that the US law provides a different bunch of tests and under FISA you have no privacy rights.

The FISA amendment 2008 snuck in a new category called “remote computing services”. This term goes back to the 1996 statute, but the definition is what we would call today cloud computing and the significance of this is that FISA (1888a) is specifically crafted to include surveillance of cloud computing from inside the data center - it is not about interception, it is about a new modality of surveillance, cloud surveillance.

Response: The safeguards for non-US citizens outside the US are indeed lower, yet they are still significant.

- **Question:** What should the EU do to mitigate the problem?

Cloud computing presents a new category of risk; we cannot assume data protection law is always technologically neutral. In the case of cloud it is not; firstly because the modality of cloud surveillance from inside the data canter - worldwide but on the US jurisdiction - is new, and secondly because the nature of the threat from US or India is also new and special in context.

The basic idea should be that in the case of cloud processing, a high level consent (after the European Citizen has been warned explicitly that he might be subject to this kind of political issues) will be necessary. The second idea would be to provide legal protections and ensure a channel towards the data protection authorities to people who can blow the whistle when they note that this is going on.

Comment: The idea of consent for decryption would require significant modifications to the French code of criminal procedure and the French internal security code. The realities of law enforcement render individual consent ideas rather unrealistic.

Comment: If we take all these conclusions about these concerns aren't we making the roll out of cloud computing in EU even more difficult? What road are we heading in if the accommodation of legislation starts eating the fabric of what the EU cloud strategy is?

Comment: With regard to data held by public authorities (which could also include personal data but could also be other strategic data) this is a show stopper. It is these issues that can make a CIO of a public administration decide to keep their own private cloud run by their own agencies and will decide not to use public cloud at all, or to a very limited extent as they cannot guarantee that law enforcements agencies from third countries will not be able to look at their data. This is down to national and regional administration level.

Conclusions

The need for some sort of common language and understanding on these technical terms and issues is necessary. If you are a micro-SME and want to take advantage of the cloud you will not be able to follow this discussion. We have to disconnect the different levels of the cloud. Cloud is not a single entity even though we talk about it as it is.

It is necessary to differentiate the needs and concerns of commercial, government and individual users of clouds, with those of the security services in a particular nation.

There will always be times where a government (or other cloud customers) will make some balanced decisions on things that it wants to put or not to put in the cloud.

We need to come to a common base of understanding and recognize what is really possible and take it on from there.

Short Speaker Bios

***Christopher Wolf**, Hogan Lovells - Christopher Wolf is a director of Hogan Lovells' Privacy and Information Management practice group. He has deep experience in the entire range of international, US and EU privacy and data security laws, including financial and health information privacy laws. He is the founding editor and lead author of the first Practising Law Institute (PLI) legal treatise on privacy and information security law. He is the founder and co-chair of a think tank devoted to emerging privacy issues, the Future of Privacy Forum. He holds a J.D. magna cum laude from Washington and Lee University School of Law, 1980.*

***Winston Maxwell**, Hogan Lovells - Winston Maxwell is a partner at Hogan Lovells and one of the leading media, communications and data protection lawyers in France. He is a member of the Bars in New York and Paris. His practice covers three principal area : telecommunications and Internet, media and entertainment, data protection and privacy. Some of his recent representative experience includes data protection advice to multinationals in the deployment of comprehensive compliance programs in Europe, as well as advising international telecommunications providers and customers on cloud computing contracts and regulations. He holds a J.D. from Cornell University Law School, 1985.*

***Jan Ostoja-Ostaszewski** joined the European Commission in 2005. During 2005-2008 he was responsible for international relations in the area of electronic communications. He was then a Member of Private Office of EU Commissioner for Information Society and Media, and EU Commissioner for Justice. In 2012 he joined Directorate-General for Justice of the European Commission where he is responsible for international relations in the area of privacy and personal data protection.*