INTERNET POLICY REVIEW
Journal on internet regulation

Volume 2 | Issue 1

Foreign clouds in the European sky: how US laws affect the privacy of Europeans

Primavera De Filippi
Research and Studies Center of Administrative Science (CERSA/CNRS), Université Paris II (Panthéon-Assas), France

Published on 18 Mar 2013 | DOI: 10.14763/2013.1.113

Abstract: This article presents a general analysis of how user autonomy in the cloud is increasingly put into jeopardy by the growing comfort and efficiency of the user-interface. Although this issue has not been, thus far, explicitly addressed by the law, it is a fundamental ethical question that should be carefully assessed to guide the future deployment of cloud computing. Different policy decisions might, in fact, significantly affect user's fundamental rights and online freedoms by shifting the balance from one part or another of the trade-off. This article aims to explore emerging trends in cloud computing technologies and analyse them from an ethical perspective to identify the issues they might raise, and the extent to which current laws and regulations actually take these issues into account.

Keywords: Foreign Intelligence Surveillance Amendments Act (FISAA), USA Patriot Act, EU Data Protection Regulation, Data sovereignty, EU Cybersecurity Directive, Cloud services, Cloud

Article information

Received: 25 Feb 2013 **Reviewed:** 13 Mar 2013 **Published:** 18 Mar 2013
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/foreign-clouds-european-sky-how-us-laws-affect-privacy-europeans

Citation: De Filippi, P. (2013). Foreign clouds in the European sky: how US laws affect the privacy of Europeans. *Internet Policy Review*, *2*(1). https://doi.org/10.14763/2013.1.113

Cloud computing provides a large number of advantages to many internet users: web-based applications such as web-mail, chats, online forums and social networks allow users to connect and communicate more easily; office productivity tools such as word processing, spreadsheets and online file storage enable users to work and collaborate with each other, without having to install any software on their own devices. Most of the perceived benefits are related to the concept of ubiquity, or the ability to access data from anywhere and at any time, regardless of the device used. Yet, these benefits come at a cost. The widespread deployment of cloud computing services provided by large multinational organisations is, indeed, source of growing concern as regards the privacy of users (Moglen, 2010; Svantesson & Clarke, 2010; Gellman, 2012).

Many cloud services are made available to the public through a common web interface (e.g, a single web page), even if they are generally provided by a variety of actors operating on an international scale. Although users are generally not concerned with the origin and location of these services, the place in which user data is being collected, stored or processed is an important element to take into account - especially in countries with stringent privacy and data protection laws (Jaeger & al, 2009). While European regulations on data protection [1] have established a common standard of protection allowing - amongst other - data to be moved freely within the EU, free flow of data beyond European borders might put the fundamental rights of EU citizens (both within and outside the EU) at risk.

CHALLENGES TO EUROPEAN DATA PROTECTION RULES

Specific attention should be paid to the legislation recently introduced in the United States, where most of the major cloud computing operators are based. In fact, despite the

Consumer Privacy Bill of Rights and other constitutional rights protecting U.S. citizens against "unlawful intrusions" on privacy "by both private and governmental actors," foreign citizens – which are not subject to the constitutional rights granted by the Fourth Amendment (Dole, 2003) – are not entitled to the same level of protection as regards the procedures for searches and seizures. Thus, U.S. laws regulating the surveillance of non-U.S. citizens through the monitoring of online communication by U.S. authorities constitute a major challenge to the enforcement of European privacy and data protection regulations.

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT) ACT

The USA PATRIOT Act – enacted shortly after the attacks of September 11, 2001 – is particularly problematic in this regard. Conceived as a means to facilitate the prevention of terrorism, it is, however, also likely to jeopardise the privacy and confidentiality of data crossing international boundaries. Indeed, several provisions of the PATRIOT Act are known to clash with various aspects of European data privacy laws insofar as they allow for U.S. authorities to legally request access to foreign personal data stored or transferred into the U.S.

Specifically, section 217 of the Act reserves U.S. government agencies the right to monitor online communications as long as previous authorisation has been granted by the owner of a "protected computer" – a term which includes systems used in "interstate or foreign commerce or communication." This essentially means that, provided that the service provider agrees, U.S. authorities could theoretically request access to any information stored in U.S.-based cloud computing platforms (such as those of Google, Apple, Amazon or Facebook) for the purpose of law enforcement. The issue was publicly acknowledged by Gordon Frazer, Microsoft U.K.'s managing director, who publicly admitted that "Microsoft cannot guarantee that EU-stored data, held in EU-based datacenters, will not leave the European Economic Area under any circumstances," and "neither can any other company" whose headquarter is subject to U.S. laws. [2].Google confirmed this statement, by subsequently admitting that the company received

numerous requests to hand over EU-citizens data to U.S. intelligence agencies - and was compelled to comply under U.S. law. [3]

In response to that, a series of legislative or institutional measures have been taken in different parts of the world (such as Canada [4], Germany [5], France [6], Spain [7] etc.) to reduce the likelihood of personal data being illegitimately exported to third countries. At the European level, the Data Protection Directive [8] (article 25) established strict rules regulating the transfer of personal data to countries outside of the European Economic Area (EEA), unless those countries have been specifically acknowledged by the European Commission as providing an adequate standard of protection. [9].While the U.S. does not belong to this category, cross-border cooperation between Europe and the U.S has been promoted by non-legislative measures and self-regulation. Most relevant in this regard are the Safe Harbour principles [10] aimed at facilitating the transfer of personal data from and to U.S. service providers (including cloud operators) which agree to comply with an adequate standard of data protection. Although based on voluntary codes of conduct, failure to comply with the agreed principles can be actioned by the U.S. Federal Trade Commission. Violations can be punished with a fine of up to $12,000 per day and persistent failure to comply could eventually lead to the institution or organisation becoming ineligible to using the safe harbour again. [11]

Yet, since most cloud operators are companies governed by U.S. law, they cannot guarantee that the data they host will not be handed over to U.S. authorities as a result of governmental requests. Many European institutions (and citizens) might thus decide to rely exclusively on cloud services provided by online operators that might preclude any attempt by foreign governments to access their personal data by ensuring that such data will only be stored and processed in European data centres. Following in the footsteps of Amazon and Microsoft, which let users select EU-based data centres in which to store their data, Google recently updated its platform to let companies only keep their data within European borders (although it does not yet allow them to select the exact location on a national basis).

THE U.S. FOREIGN INTELLIGENCE AND SURVEILLANCE ACT

The USA PATRIOT Act is only one part of the problem. Most of the safeguard measures described so far are pointless when faced with a much more intrusive (and yet, much less debated) piece of U.S. legislation: the Foreign Intelligence and Surveillance Act (FISA), which establishes special procedures for conducting physical searches and electronic surveillance of individuals allegedly involved in international espionage or terrorism against the United States of America. Enacted in 1978, the FISA was subsequently amended in 2008 with the Foreign Intelligence Surveillance Amendments Act (FISAA), which relaxed some of the requirements prescribed by the FISA, thereby facilitating the surveillance of foreign electronic communications (Title VII). Scheduled to expire on December 31, 2012, these provisions have recently been extended for another 5 years, to last until December 31, 2017.

By defining an “electronic communication service” as also including “remote computing services,” the provisions of the FISAA can now be relied upon to retrieve and inspect data or electronic communications exchanged in the realm of cloud computing. Particularly relevant for the purpose of this analysis is section 1881a, which introduces the possibility for the U.S. government to monitor foreign communication and access data of foreign citizens located

outside of the U.S., without the need for a warrant (a requirement that by virtue of the Fourth amendment, would only apply to U.S. citizens). As such, the FISAA raises important challenges to EU data sovereignty and could seriously affect the privacy of European citizens. Indeed, not only does it enable U.S. government agencies to intercept phone calls and other in-transit communications, it also allows them to request access to foreign citizens' data located in any data centre within the range of U.S. jurisdiction, without prior notice or consultation.

As Thilo Weichert, data protection officer of the German state of Schleswig-Holstein puts it, today, "*the long arm of US law stretches as far as Europe*": the FISAA could effectively force U.S. companies to disclose EU citizens' data (including personal data) without properly informing them of the matter.

While FISAA did not – until recently – receive extensive media coverage, it recently generated considerable controversy and eventually attracted the attention of European authorities. The implications of U.S. legislation on the fundamental rights of EU citizens have been recently analysed in a EU report entitled "Fighting cyber crime and protecting privacy in the cloud" [12]commissioned by the European Parliament's Committee on Civil liberties, justice and home affairs (LIBE) to analyse the impact of cloud computing on EU strategies and policies with a focus on data protection. The report examines the challenges raised by cloud computing on the right to privacy and data protection, the issues of jurisdiction, responsibility and the regulation of data transfers between countries. It emphasizes that "*where cloud computing is possibly most disruptive is where it breaks away from the forty-year-old legal model for international data transfers, jeopardising the rights of the EU citizens*." Hence, *"from a legal perspective, the challenge of jurisdiction is central."*

The report also draws attention to the potential loss of EU sovereignty deriving from the fact that data stored in any data centre operated by U.S. companies could be subject to mass-surveillance by the U.S. government: "*lack of legal certainty surrounding the [...] legal frameworks of cloud-based investigations, as well as inadequate tools to safeguard privacy and data protection increase the potential for misuses and abuses by law enforcement actors and agencies."* In this regard, Caspar Bowden (co-author of the report, and former policy adviser to Microsoft) strongly criticised the FISAA for giving *carte blanche* to U.S. government agencies which – in the name of security and the fight against terrorism – are entitled to track down any type of activities, including ordinary lawful democratic political activities that could potentially further foreign policy interests of the U.S.

The report concludes that appropriate measures should be taken to ensure that EU citizens are properly informed of the fact that personal data exported into the cloud will be more easily accessible by the U.S. government, and suggests that the violation of users' fundamental right to privacy by any online cloud operator should be considered a cyber-crime punishable under the law.

The findings of this report have been examined during a debate on cyber-security held at the European Parliament on February 20th, 2013, with a view to identify which measures should be taken to protect privacy in the cloud, in light of the recent extension of the FISAA. While recognising the dangers of the US government spying on EU citizens' data, the parliamentary committee regarded the proposed measures as being too drastic, declaring that "the basic framework of the cloud computing strategy is set and won't be changing." In particular, article 13 of the draft Cybersecurity Directive provides for the EU to cooperate with third parties for the sake of cyber-security – and such cooperation could, in theory, also include data sharing.

THE NEED FOR AN INTERNATIONAL DATA PROTECTION FRAMEWORK

While the revised European Data Protection Regulation may introduce new measures aimed at reducing the risks of EU citizens' data being handed over to the U.S. government, Sophia Veld (vice-chair of the LIBE committee and member of the Dutch social liberal party *Democraten 66*) expressed her concern that European authorities might not be properly addressing these issues by fear of standing up against U.S. authorities. Besides, the situation is further complicated by the fact that European intelligence services could actually benefit from the surveillance activities of the U.S. government in order to obtain information that they could not request under European law. [13]

At this time, therefore, in order to preserve their privacy online, European citizens shall store their data exclusively on European cloud computing platforms operated by EU-based service providers (e.g., CloudSigma, T-Systems, Gandi, or OVH, to name just a few). Such a strategy could, however, significantly slow down cloud adoption in the EU. Besides, while it constitutes a viable option for citizens living within the EU, a similar strategy cannot be implemented by non-EU residents, who are ultimately subject to the laws of the country they live in. Even the recent proposals for new data protection regulations in Europe do not indeed address the issue of potential conflicts posed by the laws of third countries.

In a global and increasingly connected online world, preserving the privacy of EU citizens might therefore require the establishment of a more comprehensive framework of international rules when it comes to privacy and data protection, but also, more generally, an improved system of internet governance, with more sophisticated models of laws and/or standards which are properly adapted and constantly updated to the latest advancements in cloud computing.

REFERENCES

Cole, D. (2002). Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens. *T. Jefferson L. Rev.*, *25*, 367.

Gellman, R. (2012). Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In *Proceedings of the World privacy forum*.

Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday*, *14*(5), 1-12.

Moglen, E. (2010). Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing.

Rauhofer, J. (2008). Privacy is dead, get over it! 1 Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*,*17*(3), 185-197.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review*, *26*(4), 391-397.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, *8*(6), 24-31.

Ward, B. T., & Sipior, J. C. (2010). The Internet jurisdiction risk of cloud computing. *Information Systems Management*, *27*(4), 334-339.

Whitaker, R. (2000), *The End of Privacy*. The New Press.

FOOTNOTES

1. See, in particular, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Directive 2002/58 on Privacy and Electronic Communications (E-Privacy Directive), as well as the General Data Protection Regulation that will eventually supersede the Data Protection Directive.

2. Speech given during the launch of Microsoft Office 365, in New York City on June 28th, 2011.

3. Statement from Google given to German media group WirtschaftsWoche on August 6th, 2011

4. In Canada, several provinces reacted to the U.S. Patriot Act by enacting and/or amending their own data protection laws so as preclude governments or organizations from transferring personal information across borders insofar as there is any risk of inappropriate disclosure for security or for commercial purposes.

5. German's Federal Data Protection Act (Bundesdatenschutzgesetz) requires all parties involved in transnational data transfers to fulfill specific requirements which are amongst the most stringent in the EU. Additional State-level restrictions have also been introduced to preserve the privacy of citizens, see e.g. the Independent Centre for Privacy Protection in Germany, requesting all institutions in the state of Schleswig-Holstein to remove Facebook social media plugins from their websites, insofar as they automatically transfers users personal data into the US, without obtaining prior informed consent.

6. In France, data transfers outside of the EEA are subject to specific requirements of consent and/or subject to prior authorisation by the Commission nationales de l'informatique et des libertés (CNIL).

7. In Spain, transfer of data offshore is only allowed into countries ensuring an adequate level of protection, or after obtaining the authorisation from the Director of the Spanish Data Protection Authority.

8. European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

9. The Commission has so far recognized only Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, and Jersey as providing adequate protection. The Commission has so far recognized only Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, and Jersey as providing adequate protection.

10. European Commission (2000), Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000/520/E, OJ L 215, 25.8.2000.

11. Such was the case of Google Inc., accused by the Federal Trade Commission of falsely certifying compliance with the U.S.-EU Safe Harbor program. Instead of charging the company, the FTC agreed to a 20 years-long settlement agreement that requires Google to undergo periodic privacy audits and to refrain from making any such misrepresentations for a period of 20 years.

12. European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), Fighting cyber crime and protecting privacy in the cloud, October 2012.

13. As Jan Phillip Albrecht, member of European Parliament working on EU data protection regulations, points out: "European intelligence services and the police are of course happy to be provided data on European citizens by the US. They could not obtain this data under European law".