Obscured by Clouds

or

How to Address Governmental Access to Cloud Data From Abroad

-

Joris van Hoboken, Axel Arnbak, Nico van Eijk[1]

Contents

1. Introduction 2
2. Governmental Access to European Cloud Data From the United States 4
2.1.1. Patriot Act, FISA and FAA 2008 5
2.1.2. Constitutional Protection and Jurisdiction under FISA 7
2.1.3. The Scope of §1881a Surveillance 10
2.1.4. Procedural Conditions Applicable to §1881a Surveillance 12
2.2. Risk Assessment of Transnational Intelligence Gathering of Cloud Data 14
2.2.1. Impact: Cloud Computing and Confidentiality Interests 14
2.2.2. Probability: Observations on Access to Cloud Data 15
2.2.3. Sharing Data Internationally, Circumventing National Safeguards? 17
2.2.4. Risk Assessment and Market Responses 18
3. Towards Addressing Governmental Access Abroad 19
3.1. The US Level: Better Safeguards in FISA for Foreigners 20
3.2. The International Law Perspective: Sovereignty and Human Rights 22
3.3. The EU perspective: Cloud Communication and Data Protection Regulation 25
3.3.1 The EU's Cloud Policy and Restrictions on Governmental Access Abroad 26
3.3.2. The EC Proposed Data Protection Regulation 27
3.3.3. The EP Amendments on Data Transfer in the General Data Protection Regulation 29
3.3.4. The In 't Veld Amendments on Transfers to Clouds Under 3rd-Country Jurisdiction 30
3.4. Improving Oversight over Transnational Intelligence Gathering in the Netherlands 32
4. Conclusion 34

[1] Institute for Information Law, Faculty of Law, University of Amsterdam, Netherlands. See: http://www.ivir.nl/staff/overview.html. The authors thank in particular Ian Brown and Douwe Korff for their comments on an earlier draft. This paper was presented at Privacy Law Scholars Conference 2013, 6-7 June, Berkeley, CA. The authors are grateful for any further comments on this draft.

1. Introduction

Governments, companies and citizens have started to move their data and ICT operations into the cloud. In this Article, we look at one specific regulatory question affecting this transition, namely the question of access to cloud data by governments abroad, national security and intelligence agencies in particular. A recent study by the authors for the Dutch education and research sector concluded that the transition to the cloud leads to a problematic decrease in overview and control over governmental access to data for law enforcement and national security purposes.[2] At the request of SURF, the Dutch organization for ICT in the higher education and research sector, the study looked into the European popular concerns about the 'PATRIOT ACT'. To do this, it analyzed the legal possibilities for U.S. governmental agencies to gain access to cloud data of Europeans in the U.S. directly through what could be called 'transnational intelligence gathering' powers, or with the legal assistance of Dutch government agencies.

As will be become clear in this Article, U.S. foreign intelligence law provides a wide and relatively unchecked possibility of access to data from Europeans and other foreigners in the cloud. The recent amendments to the Foreign Intelligence Surveillance Act (FISA) in 50 USC 1881a are of particular concern. In this Article we will discuss this provision as a primary example of lawful access to cloud data abroad (section 2.1) and use this discussion to look at the risks of transnational intelligence gathering for cloud customers (2.2).

The mere possibility that information in the cloud could be accessed by foreign governmental agencies has started to impact decision making by existing and potential cloud customers. Concerns of governmental and corporate customers spur market developments such as federated and encrypted solutions as well as 'national clouds' that are 'Patriot Act Proof'.[3] Several European Governments, including the United Kingdom and the Netherlands, have announced projects for localized clouds for the same reason. These developments consequently affect market conditions and competition, impacting U.S.-based cloud services in particular. In addition, the possibility of foreign governmental access impacts the privacy of cloud end-users and can cause chilling effects with regard to cloud computing use. When data confidentiality is found vital, the situation has led to

[2] J.V.J. van Hoboken, A.M. Arnbak & N.A.N.M. van Eijk, 'Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act', Study for SURFdirect, Institute for Information Law, November 2012, available at SSRN: http://ssrn.com/abstract=2181534.

[3] Dutch telecommunications provider KPN launched a national cloud, 'CloudNL' in September 2012, apparently informed by 'Patriot Act' concerns. In the media coverage of the launch, KPN claimed that "the Patriot Act is out of the game". "De Patriot Act staat buiten spel." Andreas Udo de Haes, 'KPN tuigt Nederlandse Microsoft-cloud op', Webwereld, 21 September 2012, http://webwereld.nl/cloud/58012-kpn-tuigt-nederlandse-microsoft-cloud-op. See also, KPN, CloudNL, https://www.kpn.com/corporatemarket/themas/cloud/cloudnl.htm. Large cloud providers also publicly complain about the Patriot Act being abused by European-based providers as a marketing tool. See e.g. Johan Leupen, Amazon-topman Vogels ziet discussie over privacy en de cloud als 'pure bangmakerij', [Interview in Dutch Financial Newspaper of Amazon CTO Werner Vogels about privacy and the cloud], Financieel Dagblad, 17 oktober 2012. And see also *infra* note 111 and accompanying text.

calls for regulatory action and termination of cloud contracts – such as in cases of medical data storage in electronic patient record systems and biometric data processing in relation to passports.[4]

The mere possibility of access to cloud data abroad has also become the subject of high-level legal and political debate, in particular in transatlantic international relations.[5] Several proposals have been made to legally address the situation of transnational intelligence gathering. This Article focuses on the question of how to address transnational intelligence gathering, again taking the FISA powers under U.S. law as an example. Regulatory solutions, from the perspective of Europe and the Netherlands in particular, are discussed on four levels. Section 3.1 discusses the possibility of limiting surveillance in the U.S. itself. Section 3.2 discusses the question of using international law as a framework to impose some limitations. Section 3.3 discusses the way in which the issue of access to cloud data is addressed in the context of the General Data Protection Regulation proposals and the EU Cloud Strategy.

We argue that ultimately the most sensible approach to address transnational surveillance would be to improve oversight over governmental access at the national and international level. Such oversight is currently mostly focused on the relation of governmental agencies towards their own residents. This stands in contrast with the increased possibilities of gaining access to data from people abroad due to the international nature of cloud service markets and communications networks. Section 3.4 discusses the way in which the oversight framework for intelligence agencies (taking the Netherlands as an example) could start to take account of emerging transnational surveillance practices.

The perspective in this paper is that of potential cloud customers in European countries that worry about the confidentiality of the information stored and processed in the cloud with respect to direct access to data in the United States. Those worries can relate to the privacy of those that the data refer to or the interests in data security of the potential cloud customer itself. In Europe, these worries are popularly discussed under the header of access under the 'Patriot Act'. A more nuanced view of relevant U.S. legislation and the history of the enactment of legal powers under U.S. law is only starting to emerge.[6] A detailed discussion of governmental access to cloud data from other jurisdictions than the United States is outside the scope of this research. At the same time, the following discussion of governmental access in the United States is illustrative for the broader issues and legal questions that are at stake.

This is not a contribution to a beauty contest between the cultures of privacy on both sides of the Atlantic. While the emphasis on the legal powers under U.S. law to spy on Europeans could make this

[4] For a discussion, see Zack Whittacker, 'Patriot Act can "obtain" data in Europe, researchers say', CBS News, 4 Dec. 2012, see: http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/.

[5] See e.g. U.S. Mission to the EU, 'Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States', Remarks by U.S. Ambassador to the EU, William E. Kennard, at Forum Europe's 3rd Annual European Data Protection and Privacy Conference, 4 December 2012, http://useu.usmission.gov/kennard_120412.html.

[6] See supra note 2. See also European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE"), 'Fighting cyber crime and protecting privacy in the cloud', prepared at the request of the LIBE Committee by the European Parliament's Policy Department of Citizens' Rights and Constitutional Affairs, with the help of the Centre for European Policy Studies and the Centre d'Etudes sur les Conflits, October 2012, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050.

impression, we want to deliberately avoid making a normative comparison. In specific areas, such as free speech related issues, U.S. law and political culture is more sensitive to civil rights and privacy than European law(s). And in certain cases specific legal standards are indeed higher. For instance, the legal standards for obtaining communications records of journalists in the United States are significantly more strict. The current debate about the overbroad surveillance of AP journalists is made possible by a notification requirement that is much weaker in most European countries, if it exists at all.[7] The protection of a variety of privacy interests under the ECHR or the EU Charter is for instance subject to a rather vague proportionality test. There are enough reasons to believe that this protection is in practice not always of the level ascribed to it by certain proud Europeans.

EU Commissioner Viviane Reding declared that no third-country legislation overrules the European privacy regulations, and that "the International Court of Justice based in The Hague is the final arbiter on disputes about access to data abroad".[8] Her statement will not be the final word on this matter,[9] but does illustrate the complex political and legal landscape associated with regulating foreign cloud surveillance.

2. Governmental Access to European Cloud Data from the United States

U.S. legislation includes a number of provisions giving governmental agencies legal powers to obtain access to data held by providers of cloud services. This section discusses the background and substance of the provision that is most striking when discussing the issue of governmental access to cloud data from a European perspective, namely Title 50, Section USC 1881a.[10] This provision provides for a possibility to gain bulk access to data on non-US persons located abroad held by electronic communications services and cloud providers.

Like in other jurisdictions, the U.S. legislation in question provides for the exercise of coercive measures to acquire data in connection with law enforcement on the one hand and national security on the other hand. In the following, we will first discuss the relevant legal powers and the protection afforded by U.S. legislation, with a specific focus on the access to cloud data under the amended Foreign Intelligence Surveillance Act (FISA). After that, we will discuss the implications for information security and the market for cloud services from a transatlantic perspective.

The following legislative instruments are considered successively: the Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), the FISA (Foreign Intelligence Surveillance Act) and the FAA (FISA Amendments Act of 2008). The focus of the Article is on foreign intelligence gathering, we do not further discuss the ECPA (Electronic Communications Privacy Act). It should be noted here that a large proportion of the provisions reflect the requirements that apply on the basis of the U.S. Constitution to the acquisition of information about *American* citizens or residents. In some cases, such as the Electronic Communications Privacy Act (ECPA), the U.S. legislator has compensated for the lack of clear

[7] See Charlie Savage & Leslie Kaufman, ´Phone Records of Journalists Seized by U.S., NYT, 13 May 2013, http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html.

[8] BBC Democracy Live, 'Data Protection Question', 15 February 2012, see [includes video]: http://news.bbc.co.uk/democracylive/hi/europe/newsid_9695000/9695923.stm.

[9] It is for instance not clear if a convincing case could be made under international legal standards. See Section 3.2.

[10] For a broader discussion of relevant provisions, including the ECPA, see supra note 2.

constitutional protection for the privacy and confidentiality of communication by setting statutory limits.

2.1.1. Patriot Act, FISA and FAA 2008

The Patriot Act was enacted in 2001 in the aftermath of 9/11. In Europe, the Patriot Act is often perceived as a law as a result of which 'data that are managed by a U.S. company can always be obtained by the U.S. authorities'.[11] This is a simplified representation of the legal state of affairs. Rather than being an independent statute, the Patriot Act is in fact a comprehensive amendment to the then existing statutory law, including FISA and ECPA. In some respects it simplified pre-existing procedures for requesting data from businesses, for example Title 50 USC, Section 1861.[12] However, the Patriot Act itself granted few new powers and mainly amended numerous other older laws in various ways.[13] The Patriot Act and the laws it amended have been amended again on a number of occasions since 2001 and some parts of it (those containing powers subject to an expiration date in the form of a so-called sunset clause) have been extended.[14] A recent extension took place on 26 May 2011.[15]

The main provisions of the Patriot Act relevant to governmental access to information are those amending the Foreign Intelligence Surveillance Act (FISA) and the Electronic Communications Privacy Act (ECPA). The FISA concerns the acquisition of foreign intelligence by wiretapping and physical and data searches. The ECPA concerns the acquisition of data from electronic communication services for law enforcement purposes. Since the amendments made by the Patriot Act, two other important amendments have been made to the FISA: the Protect America Act (PAA) of 2007 and the FISA Amendment Act 2008 (FAA 2008). These laws are of specific interest from the perspective of access to data held by cloud services. The FAA 2008 added a specific provision relating to ´Procedures for targeting certain persons outside the United States other than United States persons´ that warrants discussion from a transatlantic perspective.

---

[11] See supra note 4. The Patriot Act has been described in these terms on various occasions in the Dutch parliamentary debates. See e.g. *Dutch Parliamentary Papers II* 2010/11, 3516 (Parliamentary questions raised by member of parliament Elissen (PVV) about European data managed by American companies). *Dutch Parliamentary Papers II 2*010/11, 3514 (Parliamentary questions raised by member of parliament Schouw (D66) about an article entitled 'America rummaging about in European cloud data'). *Parliamentary Papers II* 2010/11, 3515 (Parliamentary questions raised by member of parliament Gesthuizen (SP) about the release by Google of Internet data to U.S. authorities). See also Andreas Udo de Haes, 'Amerika graait in Europese clouddata', Webwereld, 1 July 2011, http://webwereld.nl/nieuws/107156/amerika-graait-in-europese-clouddata.html. Notably, concerns over the Patriot Act are not new and not restricted to Europe. See e.g. Information & Privacy Commissioner for British Columbia, 'Privacy and the USA Patriot Act, Implications for British Columbia Public Sector Outsourcing', October 2004.

[12] For further discussion and references, see supra note 2. The PATRIOT ACT, Title II, Section 220, made it possible to obtain a national search warrant for electronic evidence from a federal court, whereas it had previously been necessary to obtain warrants in each state concerned. See Department of Justice, 'USA PATRIOT Act: Sunsets Report', April 2005, http://www.justice.gov/olp/pdf/sunsets_report_final.pdf.

[13] See Orin S. Kerr, 'Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't', 97 Northwestern University Law Review 2003, pp. 607-608.

[14] Examples are the USA PATRIOT Improvement and Reauthorization Act of 2005, the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, An Act To Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005, the FISA Sunsets Extension Act of 2011 and the USA PATRIOT Sunsets Extension Act of 2011.

[15] The PATRIOT Sunsets Extension Act of 2011 (H.R. 514) Pub. L. 112-14 (26 May 2011).

Below follows a discussion of the conditions under which relevant governmental agencies have the statutory power under FISA to gain access to data of European cloud customers. Analysis of how these data are further processed and exchanged, and the specific government entities and officers that play a role in these practises, is a concern beyond the scope of this study. And of course, there is only limited information available about actual interdependencies and collaboration between the various organizations and officials such as the Attorney General, the Director of National Intelligence, the NSA, the U.S. Marshals, the FBI and the CIA and the extent to which their remits overlap.[16]

Within the U.S. statutory framework the FISA provides for the acquisition of foreign intelligence information (50 USC §1801-1885c) by U.S. authorities.[17] The Patriot Act has amended the statutory powers in various ways. The same is true of the FISA Amendments Act (FAA) of 2008.[18] The FAA 2008 is of particular importance for governmental access to cloud data from foreigners. It introduces new provisions regulating the power of U.S. government entities that gather foreign intelligence information for national security purposes to acquire data of non-U.S. persons believed to be located abroad.[19] These provisions can be found in Section 702 of the FAA 2008 and the section thus added to Title 50 USC §1881a (in Title VII – 'Additional procedures regarding certain persons outside the United States') and are explained below. The U.S. Government may also obtain information from the intelligence services of foreign nations and conducts human and technical surveillance programs that are governed by Executive Order 12333 (as amended) that are exempt from FISA safeguards altogether.[20]

The significance of Title 50 USC §1881a for Europeans and other non-U.S. persons located abroad can best be understood by looking at a combination of three elements. The first is the constitutional protection of U.S. persons and the lack of such protection for non-U.S. persons located outside the United States (discussed in more detail section 2.1.2). Second and related, one has to look at the background to the FISA, namely the wish to introduce a system of oversight over the acquisition of intelligence information, in view of its possible impact on the fundamental rights of U.S. persons. And third, it is important to understand that the FAA 2008 amendments to the FISA were a codification and legalization of the illegal and warrantless wiretapping program of the electronic communications of U.S. citizens by the Bush administration.

The original FISA dates from 1978 and introduced a statutory framework for the gathering of foreign intelligence information by electronic surveillance. This framework was a reaction to abuses committed by U.S. intelligence agencies and the resulting framework is a compromise between two conflicting interests: on the one hand, the wish to facilitate the acquisition of foreign intelligence by

[16] The Washington Post recently published a study of the complex interplay between the intelligence and security agencies in the United States. See The Washington Post, 'Top Secret America', 2011, http://projects.washingtonpost.com/top-secret-america/.

[17] For a concise overview of the provisions of the FISA, see CRS, 'The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview',
24 January 2007, http://www.fas.org/sgp/crs/intel/RL33833.pdf.

[18] And the Protect America Act of 2007, which was replaced by the FAA 2008.

[19] For a study containing an overview (for the European Parliament) of the implications of this provision from a European perspective, see supra note 6.

[20] See Clapper v. Amnesty 568 U.S. ___ (2013). This Executive Order allows the executive to conduct surveillance operations abroad. See Executive Order No. 12333, §§1.4, 2.1–2.5, 3, 1981.

the authorities in the interests of U.S. national security and, on the other, the wish to ensure the applicable constitutional protection in relation to the acquisition of foreign intelligence information, insofar as this could relate to communications of U.S. persons.[21] The FISA, it is consistently argued, was therefore not intended to protect Europeans or other foreigners from the interception of their communications by U.S. intelligence and national security agencies.[22] Nor was it ever intended that the FISA should regulate the interception of communications of foreigners not located within U.S. territory.[23]

The FAA 2008 is the outcome of a more recent debate in the United States on warrantless wiretapping by the NSA during the George W. Bush administration. The U.S. government had intercepted the communications of Americans without obtaining a judicial warrant, as was first reported by The New York Times in late 2005.[24] The subsequent debate focused on whether there had been unconstitutional wiretapping of American citizens on the pretext of gathering foreign intelligence. In response, the U.S. legislator modernized the FISA and regulated these controversial activities by introducing the Protect America Act (PAA) in 2007 and the FAA in 2008, replacing the PAA. In the U.S., the FAA 2008 was and remains controversial due to its impact on the civil liberties of U.S. citizens and its alleged circumvention of constitutional protection. Another controversial aspect of the FAA 2008 is that it provided immunity for the industry that had participated in Bush-era warrantless wiretapping. It should be noted that the FAA 2008 is not controversial in the United States insofar as it really does only concern the collection of foreign intelligence about foreigners located abroad.[25] The debate in the United States instead focuses on the issue of whether the exercise of wiretapping powers and powers to obtain data about people outside the United States could jeopardize the fundamental rights of *Americans*. In the end of 2012, the FAA 2008 has been extended.[26] In early 2013, the U.S. Supreme Court dismissed a constitutional challenge of the FAA 2008 by a number of American organizations and citizens for a lack of standing.[27] The Court considered the claims by lawyers and human rights workers that their communications were likely intercepted as a result of §1881a surveillance (without a warrant) too speculative.[28]

2.1.2. Constitutional Protection and Jurisdiction under FISA

[21] See William Banks, 'The Death of FISA', 91 Minnesota Law Review 1209, 2007, pp. 1216-1233.

[22] See e.g. McDonnell (Director of National Intelligence), Modernizing the Foreign Intelligence Surveillance Act', Statement for the Record, Senate Select Committee on Intelligence, May 1, 2007, (stating that proposals in US Congress: "[seek] to restore FISA to its original focus on protecting the privacy interests of persons in the United States."

[23] See Stephanie C. Blum, 'What Really Is at Stake with The FISA Amendment Act of 2008 and Ideas for Future Surveillance Reform', 18 Public Interest Law Journal, 2009., pp. 278-279.

[24] See James Risen & Eric Lichtblau, Bush Lets U.S Spy on Callers Without Courts, The New York Times, 16 December 2005, http://www.nytimes.com/2005/12/16/politics/16program.html. For an overview see William Banks, 'Programmatic Surveillance and FISA: Of Needles in Haystacks', 88 Texas Law Review 1633-1667, (2010) , at 1641-1643. See also supra note 23; John Cary Sims, 'What NSA is Doing... and Why It's Illegal', 33 Hastings Constitutional Law Quarterly 101 (2006).

[25] See supra note 23, pp. 295-296.

[26] See Bill Chappell, 'President And Congress Extend FISA Wiretapping Act To 2017', 28 December 2012. See also The Washington Post 2012. See also The Washington Post, 'Oregon senator blocks five-year extension of surveillance law', 11 June 2012.

[27] *Clapper v. Amnesty* 568 U.S. ___ (2013). For the backgrounds of this challenge, see ACLU, 'Why the FISA Amendments Act is Unconstitutional', 5 February 2008, http://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf..

[28] For further discussion, see Section 3.1.

There are two elements that could, in theory, restrict the scope of legal powers provided for in FISA to gather information about Europeans. First, one can imagine a general restriction following from the U.S. constitutional protection against unreasonable searches and seizures in the Fourth Amendment. And second, one could imagine a general restriction not to gather data that are not on U.S. territory, or of people with no relation to the U.S., following from the jurisdictional scope of the legal powers provided for in FISA. As it turns out, however, both these possible types of restrictions do not materialize in practice. First, the Fourth Amendment does not apply to lawful access to cloud data of non-U.S. persons located abroad. Second, the legal power in question is designed to be used in respect to services that hold data of or about non-U.S. persons located abroad regardless of where the data is stored. As further discussed below, any cloud or communications service that conducts continuous and systematic business in the United States can in principle be the subject of a request for data of non-U.S. persons located abroad. They do not need to have headquarters in the U.S. to be subject to legal powers in FISA, neither does it matter under U.S. law whether the data is stored on a foreign territory and/or subject to privacy and confidentiality laws or other restrictions under the laws of countries where the data resides.

The right to protection from unreasonable searches and seizures is contained in the Bill of Rights in the Fourth Amendment to the U.S. Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[29]

This protection applies if a person has a 'reasonable expectation of privacy'.[30] However, it is limited by what is known as the 'Third Party doctrine'.[31] If one hands over information to a third party, such as a financial service provider, one can no longer, in principle, have any reasonable expectation of privacy with regard to this information.[32] The constitutional protection afforded by the Fourth Amendment thus ceases to apply in situations in which data are managed by third parties. This obviously limits the relevance of the Fourth Amendment to the cloud environment and the networked digital world significantly.[33]

However, from the perspective of Europeans and other non-U.S. persons abroad using cloud services that fall within U.S. jurisdiction there is even a bigger problem than the Third Party Doctrine: the Fourth Amendment is entirely inapplicable. The Fourth Amendment can only be invoked by U.S. citizens and by foreigners who have developed such ties with the United States that they form part of the national community. As the Supreme Court held in the case of *United States v. Verdugo-Urquidez*:

[29] United States Constitution, Bill of Rights, adopted 1791.

[30] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[31] *Id*. At 361. See also *United States v. Miller*, 425 U.S. 435, 443 (1976).

[32] See also Daniel J. Solove, *The Digital Person*, New York: NYU Press, 2004, pp. 200-209.

[33] For a discussion of this matter see e.g. Orin S. Kerr, 'A User's Guide to the Store Communications Act - and a Legislature's Guide to Amending It', 27 George Washington Law Review 2004, p. 3.

> There is […] no indication that the Fourth Amendment was understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory or in international waters.[34]

This means that foreign 'users' of U.S. cyberspace who have no other connections with the United States are, in principle, not entitled to the protection of the Fourth Amendment.[35] The debate in the American scholarly literature on the precise nature of Fourth Amendment protection in the cloud environment is therefore irrelevant for the discussion of governmental access to data in the cloud in this paper.[36] A stipulation that "acquisitions under §1881a must comport with the Fourth Amendment" may sound comforting, but is immaterial for foreign cloud customers.[37]

In its decisions, the Supreme Court has indicated that comparable protection for non-U.S. persons located abroad (i.e. comparable to that of the Fourth Amendment) will have to be imposed through other political or legislative channels:

> If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.[38]

Whether international law and specific treaties already limit the ability of the United States government to gather access to information about non-U.S. persons located in Europe, will be further discussed in section 3.2. At this point, it suffices to say that there is nothing in the FAA 2008 or the legal literature in the U.S. that suggests that international law is a limiting factor under U.S. law.[39]

The question of who is subject to U.S. jurisdiction is answered in case law, for example in decisions on access to data at foreign banks that conduct business in the United States. As soon as there can be said to be systematic and continuous activities within the borders of the United States', U.S. law applies in principle.[40] If a company is a subsidiary or branch of a U.S.-based company, or if it has one in the United States, it may be assumed that such jurisdiction exists, but jurisdiction may also exist in other more complex cases. A recent report on cloud computing summarizes the position as follows:

> The United States […] takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject U.S.

[34] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990).

[35] See Banks 2010, pp. 1656-1657 (*supra* note 24).

[36] See, for example, Banks 2010 (*supra* note 24), fn. 23 and accompanying text ("*The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the United States if the surveillance involves U.S. persons who do not have a connection to a foreign power*.").

[37] *Clapper v. Amnesty* 568 U.S. ___ (2013)("*Although the foreign client might not have a viable Fourth Amendment claim […] it is possible that the monitoring of the target's conversations with his or her attorney would provide grounds for a claim of standing on the part of the attorney*.").

[38] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 275 (1990).

[39] See generally, Curtis Bradley, *International Law in the U.S. Legal System*, Oxford University Press, 2013. For a discussion, see also *infra* Section 3.2.

[40] See e.g. *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984) "The foreign origin of the subpoenaed documents should not be a decisive factor.").

> jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.[41]

In any event, the location where the data are stored is not decisive for determining whether a cloud provider is subject to FISA jurisdiction and statutory powers concerning access to data. This can bring U.S. law into conflict with the law of other countries that tie restrictions to the export of data to other territories (such as the EU data protection rules).[42] In response to the parliamentary debate in the Netherlands on biometric data of Dutch citizens held by a company that was a subsidiary of an American company, the Dutch Minister of the Interior came to a similar conclusion. The (highly sensitive) data could, in theory, be demanded by U.S. government authorities. And the possibility also exists in relation to associated companies with activities in the United States if these companies possess, keep or control the data concerned.

2.1.3. The Scope of §1881a Surveillance

Title 50 U.S.C. §1881a is the statutory provision under which U.S. intelligence agencies can gather foreign intelligence information about foreigners abroad.[43] The §1881a surveillance power rests with the Attorney General and the Director of National Intelligence. They may jointly authorize the targeting of persons reasonably believed to be located outside the United States. The authorization can involve the assistance of electronic communication service providers and can be given for a period of up to one year. The §1881a surveillance can take place through different kinds of electronic communication service providers, including telecommunications carriers, providers of electronic communication services and providers of remote computing services.[44] Remote computing services are defined as "the provision to the public of computer storage or processing services by means of an electronic communication system", thereby including cloud service providers.[45] The FAA 2008, unlike the FISA, is claimed to be technology-neutral.[46] Under the FAA, it no longer makes any difference what technology is used to transmit the intercepted data; both open transmission over the airwaves by satellite and closed transmission by optical cables therefore come within the scope of this provision.

On a close look, there are hardly any substantive limitations to §1881a surveillance that can be considered relevant in relation to non-U.S. persons located abroad. The most important would be that such surveillance must be aimed at gathering foreign intelligence information.[47] However, this term is broadly defined. It comprises information relating to a foreign power or region in connection

[41] See Hogan Lovells, 'A Global Reality: 'Governmental Access to Data in the Cloud', Washington, DC, 23 May 2012, http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf, p. 5.

[42] For further discussion, see Section 3.3.

[43] For a concise explanation of this provision by the U.S. authorities themselves, see James R. Clapper and Eric H. Holder, 'Letter to (U.S. Congress) John Boemer, Harry Reid, Nancy Pelosi and Mitch McConnell about the re-authorization of Title VII of the Foreign Intelligence Surveillance Act (FISA) enacted by the FISA Amendments Act of 2008 (FAA)', 8 February 2012, http://www.justice.gov/ola/views-letters/112/02-08-12-fisa-reauthorization.pdf.

[44] See 50 USC 1881(4). Unlike traditional FISA, "*§1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur*." See Clapper v. Amnesty 568 U.S. ___ (2013).

[45] See 18 USC 2711(2).

[46] See also Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws', 88 Texas Law Review 1685 (2010).

[47] For the definition of foreign intelligence information, see Title 50 USC, Section 1801(d).

with national defense, national security or acts relating to the foreign affairs of the United States.[48] Thus, §1881a surveillance is not restricted to intelligence gathering in relation to foreign national security threats for the United States, or the fight against terrorism even though in the discussions in U.S. Congress may sometimes suggest otherwise. FISA §1881a surveillance can also relate to the gathering of intelligence related to U.S. political, economic and strategic interests more broadly. A European Parliament study recently clarified that "it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US Clouds."[49]

In addition, the acquisition of foreign intelligence information need not be the only or primary purpose. It is sufficient if obtaining such information is a significant purpose of the surveillance.[50] This test has become less strict following the enactment of the FAA 2008.[51]

> In addition, non-U.S. person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.[52]

Banks summarizes the significance of §1881a surveillance as follows:

> "Although details of the implementation of the program authorized by the FAA are not known, a best guess is the government uses a broad vacuum-cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then NSA engages in a more particularized collection of content after analyzing mined data."[53]

To conclude, §1881a is a statutory procedure that allows the broad, programmatic, sweeping catch-all acquisition of data about foreigners. The acquisition need not be targeted at specific persons or the specific content of their communication, as long as it somehow contributes to the collection of foreign intelligence information.[54] The power can be used in relation to cloud computing services conducting business in the United States. This is not contrary to the U.S. Constitution. As long as the risk of capturing data of U.S. persons under a specific §1881a authorization is minimized, the amount

[48] The ACLU states, for example, that it can concern "journalists, human rights researchers, academics, and attorneys [...] Think [...] of an academic who is writing about the policies of the Chávez government in Venezuela, [...]." See ACLU 2008 (*supra* note 27).

[49] European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE"), 'Fighting cyber crime and protecting privacy in the cloud', prepared at the request of the LIBE Committee by the European Parliament's Policy Department of Citizens' Rights and Constitutional Affairs, with the help of the Centre for European Policy Studies and the Centre d'Etudes sur les Conflits, October 2012, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050. For a discussion of the boundaries of foreign intelligence operations under U.S. law, see also Phillip R. Trimble, *International Law: United States Foreign Relations Law*, New York: Foundation Press, 2002, pp. 247-259.

[50] See 50 USC 1804(a)(6)(b). See also Richard H. Seamon & William D. Gardner, 'The PATRIOT Act and the Wall between Foreign Intelligence and Law Enforcement', 28 Harvard Journal of Law and Public Policy 324 (2005).

[51] For a discussion see Fletcher N. Baldwin & Daniel R. Koslosky, 'Mission Creep in National Security Law', 114 West Virginia Law Review 719-720 (2011).

[52] Banks 2010, p. 1646 (*supra* note 24).

[53] Banks 2010 (*supra* note 24).

[54] *Id.* See also LIBE 2012 (*supra* note 49).

of data that can be collected of Europeans or other non-U.S. persons located abroad appears essentially unlimited.

2.1.4. Procedural Conditions Applicable to §1881a Surveillance

There are a number of procedural conditions and reporting obligations applicable to §1881a surveillance and FISA surveillance more generally. From the perspective of non-U.S. persons located abroad, however, these conditions do not restrict the possibility of U.S. governmental agencies to acquire or further process their data.

Surveillance authorized under §1881a is subject to approval of the special Foreign Intelligence Surveillance Court (FISC). This approval must be given beforehand by the FISC.[55] Notably, both §1881a surveillance as well as its necessary FISC approval is programmatic. There is no requirement for a separate judicial approval of the FISC for each 'individual exercise' of §1881a. The FISC approval relates to the annual certifications by the Attorney General and the Director of National Intelligence which identify the targets of the acquisition of foreign intelligence information.

The procedural safeguards for non-U.S. persons located abroad are weaker than before the introduction of the FAA 2008. Before, the U.S. authorities had to show in each individual case, that the target of the acquisition was a foreign power or an official of such a power, and on this basis obtain the FISC's approval.[56] This meant in practice that in cases of this kind the American authorities afforded the same legal protection to non-U.S. persons located abroad as to persons in the United States, although no such protection exists under the U.S. Constitution. In defense of the weaker safeguards of FAA 2008, U.S. governmental officials consistently point out that the former restrictions are inappropriate for foreigners:

> "Although FISA' s original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government's acquisition of vital information, without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 [§1881a] has significantly increased the Government's ability to act quickly."[57]

It is worth noting that this wording wrongly suggests that §1881a surveillance has to be targeted to specific persons overseas that are suspected of grave wrongdoing. §1881a surveillance does not have to be restricted to 'terrorist suspects overseas' in such manner.

The procedural safeguards and FISC supervision under §1881a are aimed at ensuring the constitutional protection of Americans and persons in the U.S. For example, the review by the FISC is intended to ensure that i) the power is exercised in relation to non-U.S. persons located outside the U.S., (ii) the limitation in respect of the lawfulness of the acquisition of communications that are entirely within the United States is observed, and iii) the procedures for the exercise of the power by

[55] Unless there are exigent circumstances. See 50 USC 1881a(i)(3)), 1881a(c)(2).

[56] *Supra* note 43, p. 4.

[57] *Id*., p. 4. Notably, §1881a surveillance does not have to be restricted to 'terrorist suspects overseas'. This wording also suggests that §1881a surveillance has to be targeted at actual suspects.

the U.S. authorities are consistent with the requirements of the Fourth Amendment.[58] It follows that the judicial review by the FISC actually does not provide any legal protection for non-U.S. persons located abroad. There is no possibility for FISC to check whether the acquisition of information about foreigners and the subsequent impact on their privacy is proportional to the purpose of U.S. foreign intelligence gathering. Thus, even if a cloud service feels it is being confronted with unreasonable bulk data requests, it has no hook to complain about this at the FISC. This, in combination with the general lack of acknowledgement of privacy interests of foreigners in the general U.S. discourse about foreign surveillance, can only lead to the conclusion that there is no reason for U.S. government agencies to ensure that §1881a surveillance takes the privacy interests of people abroad seriously.

Owing to the nature of intelligence operations little information is available about how §1881a surveillance takes place in practice. The information about the exercise of the power is not in the public domain.[59] Considering the programmatic character of the approval of §1881a surveillance, the number of FISC approvals sought is not indicative of the impact on the civil liberties of non-U.S. persons. Thus, even if such specific numbers were reported they would not be of much use. Besides review by the FISC there are also the mandatory half-yearly internal reports on the acquisition of data on the basis of §1881a. However, these reports are secret and are sent only to the special committee for national security in Congress and to the FISC.[60] The public reporting obligation in the FISA does not extend to numbers on the use made of §1881a. As a result of these public reports, it is known, for example, how often the power to gain access to business records (50 USC § 1861) is exercised in the US.[61]

Perhaps the most telling problem for cloud customers is the impossibility to organize transparency about governmental data requests in their relations with cloud providers, contractually organizationally, or technically. When cloud services receive requests for data by intelligence agencies they will typically be under an obligation to keep this strictly secret from their respective customers. The FISA and §1881a is no different in that regard. It even makes it possible to put services under an obligation

> "to provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of

[58] *Clapper v. Amnesty* 568 U.S. ___ (2013).

[59] For a Dutch study discussing the structure of the review of intelligence and security services see Review Committee on the Intelligence and Security Services, 'Accountability of intelligence and security agencies and human rights', The Hague, 2007.

[60] Heavily redacted versions of these reports have been made public as a result of FOIA requests. See, for example, Attorney General and the Director of National Intelligence, 'Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', (Reporting Period: Jun 1, 2009 - Nov 30, 2009), May 2010, available at http://www.fas.org/irp/agency/doj/fisa/sar-may10.pdf.

[61] This happened 205 times in the 2011 calendar year. See Department of Justice, Report submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act, 30 April 2012, http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf. The obligation to publish these data is a consequence of 50 USC 1862(c)(1). See more recently EPIC, '2012 FISA Orders Up, National Security Letters Down, No Surveillance Request Denied', 2 May 2013, http://epic.org/2013/05/2012-fisa-orders-up-national-s.html; EPIC, 'EPIC FOIA Request Reveals Details About Government Cybersecurity Program', 24 April 2013, http://epic.org/2013/04/epic-foia-request-reveals-deta.html.

> interference with the services that such electronic communication service provider is providing to the target of the acquisition."[62]

In other words, if transparency about access to data for cloud customers were to be built into the architecture, the provider could be put under an obligation to build a backdoor into such technological protection measures. Contractual obligations on cloud providers to resist requests with all legal means or to be as transparent as possible do have some value. But ultimately, the impossibility to build a trust relationship about access to data by governmental agencies between cloud customer and provider is exactly the problem for potential cloud customers that worry about access to their data abroad.

2.2. Risk Assessment of Transnational Intelligence Gathering of Cloud Data

In this section, we assess the risks of the current legal framework for information security and data confidentiality interests of cloud customers in Europe. We will first look at the impact of transnational surveillance of cloud data. In the absence of official documentation on such practices, the subsequent sections on their probability and data sharing practices between intelligence agencies are of a more conceptual nature, based on relevant market, technological and intelligence gathering trends.

It is important to differentiate data requests for intelligence purposes from those activities undertaken by law enforcement agencies that seek to resolve crime. The exercise of power by law enforcement agencies ('LEAs') is usually concentrated on criminal offenses occurring within their jurisdictional borders, and LEAs should use Mutual Legal Assistance Treaties ('MLATs') when requesting data from LEAs in other countries.[63] Intelligence agencies, on the other hand, have an inherently broader interest, for example aimed at the spheres of prevention of certain types of events, political surveillance and furthering economic interests of the state.[64] As we will see in section 2.2.2, intelligence agencies share data with each other on a strategic basis ('quid pro quo'). Due to these substantially different aims and data acquiring practices,[65] legal systems differentiate between the two. In the context of cloud computing surveillance, however, policymakers seem to systematically confuse intelligence and law enforcement practices (see section 3.3). In this section, we retain our focus on access to data for intelligence gathering purposes, such as the surveillance made possible by FISA's §1881a.

2.2.1. Impact: Cloud Computing and Confidentiality Interests

[62] See 50 USC 1881a.

[63] See Agreement on mutual legal assistance between the European Union and the United States of America', L 181/34, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF. See Council of Europe, Venice Commission, Report on the Democratic Oversight of the Security Services, Adopted by the Venice Commission At its 71s Plenary Session (Venice, 1-2 June 2007), http://www.statewatch.org/news/2007/jun/venice-com-control-of-security-services.pdf. Whether or not these MLATs are used in practise is the topic of discussion. For further discussion, see also Section 3.2.

[64] Clear examples of the broader scope of intelligence surveillance activities are the wide definition of 'foreign intelligence information' and 'significant purpose' discussed in Section 2.1.3.

[65] The legal separation between intelligence and law enforcement practises is blurring, however. In the U.S., for example, data gathered for intelligence purposes is increasingly used in criminal investigations and police departments are starting their own intelligence operations. For a discussion, see *supra* note 51.

The greatest impact of the transition to the cloud revolves around the conditions under which such access can take place. The mere possibility that information in the cloud could be accessed by foreign governmental agencies under the current legal provisions has an obvious impact on the confidentiality, autonomy, control, intellectual freedom and information position of cloud customers. Customers can never be sure exactly how cloud providers process their data when faced with governmental data requests, and cannot inform themselves whether or not cloud providers cooperate closely with government entities when it comes to intelligence gathering.[66] This problem is also recognized by cloud providers. Consider for instance Amazon's CTO Werner Vogels reaction in the Dutch debate about privacy in the cloud. While trying to dispel worries about access to data under U.S. law, he acknowledged that Amazon informs their customers if there is a request for data, "unless there is a duty to keep it secret".[67]

It remains to be seen, moreover, whether customers ever have complete insight into the 'activities of a cloud provider in the United States' (in the case of non-U.S. companies), into the activities of their respective business partners, into actual removal of data from the servers of cloud providers (and their business partners) at the request of end users and into what happens with the stored data in the event of bankruptcy, a takeover or if they wish to end the agreement. True confidentiality in the cloud is clearly hard to achieve, thereby also creating commercial and shareholder risk.

To put such confidentiality concerns of the cloud in perspective, the act of communicating in itself limits the possibility to protect data against access requests for intelligence purposes.[68] What exactly is at stake when cloud data are accessed also depends on various other factors, such as the different types of data. Some are sensitive due to the insight they can provide into (segments of) a foreign population.[69] Such sensitive data for intelligence gathering extend far beyond the data that are considered 'personal' (research data sets, state and corporate secrets, etc.).[70] The impact of access to cloud data for intelligence purposes also depends on the cloud customer concerned. Most organizations responsible for the confidentiality concerns of their customers or citizens face substantial confidentiality concerns when deciding to entrust data to cloud computing, in particular when end-users rely on their storage and processing policies. Other companies and government agencies will seek to safeguard their strategic interests, intellectual property, employee data and business or government secrets and may actually want to cooperate with intelligence agencies and deem this in their self-interest.[71]

2.2.2. Probability: Observations on Access to Cloud Data

[66] A recent example is the ruling of the District Court Virginia in *EPIC v. NSA* concerning the cooperation between Google and the NSA. The court ruled that neither Google nor the NSA needed to confirm or deny whether they cooperate. See *EPIC v. NSA*, 11-5233 (6th Circuit 2012), available at http://www.wired.com/images_blogs/threatlevel/2012/05/EPIC-v.-NSA-DC-Cir.-2012.pdf. See also David Kravets, 'Court Upholds Google-NSA Relationship Secrecy', Wired.com, 11 May 2012, http://www.wired.com/threatlevel/2012/05/google-nsa-secrecy-upheld/.

[67] See e.g. *supra*, note 3 Leupen 2012.

[68] See *supra* note 2.

[69] Including, but not limited to: identity and biometric data, medical data, financial data, electronic communication data, data from and about politicians, journalists, government officials, political and religious groups and data about the whereabouts and mobility patterns of the population.

[70] This aspect is insufficiently taken into account within current EU policymaking, see Section 3.3.

[71] The Dutch General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) is actively offering assistance to such organizations. See: https://www.aivd.nl/onderwerpen-0/cyber-security/taak-aivd/.

In its report about the advantages and risks of cloud computing, the European Network and Information Security Agency (ENISA) estimated the probability of foreign access to cloud data and deemed the associated information security risks to be 'high'.[72] Note in this respect that in 2009, ENISA still assumed that the physical location of information storage determines the scope for data access by governmental agencies. Since 2009, the adoption of cloud services is growing spectacularly. As a result, more and more data can be retrieved from the cloud. The value for intelligence agencies of direct access to data through cloud providers is obviously increasing, but its scale is a much harder aspect to assess due to the more covert nature. Official information is hardly available on this subject, we base our assessment of such probability on technical, market and intelligence surveillance practice developments.

Traditional means of lawful access to communications through wiretapping are becoming less effective. Important causes are the rise of web based communications and the more recent rise of encryption in real-time communications. Conventional telecommunications providers are required by law to set up their networks to facilitate lawful access to data and wiretapping.[73] For webmail and social network providers, HTTPS communication is becoming standard practice, so communication cannot be effectively intercepted in transit except at these providers directly.[74] End-to-end encryption on the web implies that such communication does not always become effectively accessible through communications carriers. U.S. scholar Swire states that the attention of intelligence and law enforcement agencies as a consequence will shift to cloud services where the actual storage and processing of those communications will take place. Contrary to transit, the information stored on their servers is no longer encrypted, as it has to be accessible for end-users and is often analyzed for commercial purposes.[75] Indeed, on 20 March 2013 the FBI General Counsel called for legislation to provide public authorities real-time access to information stored in the cloud.[76]

---

[72] See European Network and Information Security Agency, 'Cloud Computing Risk Assessment', 2009, p. 45-46, http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[73] But already in 2005, the usefulness of traditional wiretapping schemes was declining due to the rise of IP-based (packet-switched) communications. See TILT & Dialogic, 'Aftapbaarheid van telecommunicatie, Een evaluatie van hoofdstuk 13 Telecommunicatiewet', Tilburg, november 2005, p. 67-69, http://www.dialogic.nl/documents/2004.59-0535.pdf.

[74] C. Soghoian, 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era'. 8 J. on Telecomm. and High Tech. Law 359 (2009), p. 386. See also Peter R. Swire, 'From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud', International Data Privacy Law, 2012, Vol. 2, No. 4, p. 7-10.

[75] See Swire 2012 (*supra* note 74), p. 10. Perhaps in response to such commercial pressure, information will increasingly be encrypted by cloud users. On the other hand, technical complications, costs, key management and commercial incentives remain serious drawbacks to the wide adoption of encrypted data storage in the cloud. And the White House has recently been backing plans to overhaul wiretapping legislation and create new powers to require backdoors into encrypted communications. See Charlie Savage, U.S. Weighs Wide Overhaul of Wiretap Laws, The New York Times, 7 May 2013, http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html.

[76] See A. Weissmann, 'New Technologies, National Security, and the Law', American Bar Association, Standing Committee on Law and National Security, 20 March 2013, video available at http://www.c-spanvideo.org/program/311627-1&showFullAbstract=1. See also Mathew J. Schwartz, FBI Seeks Real-Time Facebook, Google Wiretaps, Information Week, 1 May 2013, https://www.informationweek.com/security/privacy/fbi-seeks-real-time-facebook-google-wire/240154011. For an argument about the security flaws of demanding backdoors and wholesale wiretap capabilities in communications architectures, see S. Landau, '*Surveillance or Security*?', MIT Press: Boston, 2010.

Since there is no actual transparency about actual requests, policymakers can still downplay the risks that cloud data or communications are retrieved by intelligence agencies.[77] But recent reports may justify claims that bulk access to cloud data for intelligence purposes either already is or soon will be soaring.[78] Examples include a much discussed new NSA analysis center that can potentially collect all information relevant to the United States interests.[79] The Chief Technology Officer of the CIA recently stated (for recruiting purposes) that "it is nearly within our grasp to compute on all human generated information", with the aim of "protecting and advancing America's interests."[80]

On a more conceptual level, dramatically increasing data collection and processing practices in the private sector further enhance the perceived increase in cloud surveillance. Intelligence agencies and law enforcement can and do rely on private sector data, collected for commercial purposes (with sometimes lower legal safeguards), to fuel their own big data operations. Already described as 'the invisible handshake' by Birnhack and Elkin-Koren in 2003,[81] or the 'surveillance assemblage' by Haggerty and Ericson,[82] it has become evident that availability of data in the private sector and accessibility for government purposes are interdependent: without such data storage and processing practices in the private sector, the intrusion into the private sphere by public authorities through data gathering would be restricted – and perhaps confined to more targeted operations. Where specific data sets have been made subject to obligations to keep the data available in the private sector in the past – such as electronic communications data retention – today abundant data availability in the cloud context makes intelligence gathering more valuable and lowers transactions costs for access as cloud providers function become a one-stop shop for data.

2.2.3. Sharing Data Internationally, Circumventing National Safeguards?

Another important question to address is the extent to which U.S. intelligence agencies have a reason to gather intelligence about Europeans directly in the United Sates, while they could also gather such intelligence with the cooperation of their European counterparts.[83] A 2009 report by the Dutch Review Committee on the Intelligence and Security Services ('CTIVD') offers some insight in the cooperation between and data sharing practices of intelligence agencies internationally.[84] The report interestingly observes that day to day data sharing between agencies is mediated by the

[77] See *supra* note 5.

[78] See Section 2.1.3. On the "changing economics of surveillance", see also Soghoian 2009 (*supra* note 74), pp. 384-387

[79] See Swire 2012 (*supra* note 74), p. 8. See also J. Bradford, 'The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)', Wired.com, 15 March 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

[80] See Michael Kelly, 'CIA Chief Tech Officer: Big Data Is The Future And We Own It', Business Insider, 21 March 2013, http://www.businessinsider.com/cia-presentation-on-big-data-2013-3.

[81] M. Birnhack & N. Elkin-Koren, 'The Invisible Handshake: The Re-emergence of the State in the Digital Environment', 8 Virginia Journal of Law & Technology 2003.

[82] See also Kevin D. Haggerty and Richard V. Ericson, 'The Surveillant Assemblage'. British Journal of Sociology, Vol. 51, nr. 4 (2000), pp.605 – 622.

[83] In comparison with extraterritorial and/or human intelligence gathering abroad, transnational surveillance is less risky. See e.g. Mukasey and McConnell, 'Letter to the House Permanent Select Committee on Intelligence', 22 October 2008.

[84] CITVD, 'De samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten', CTIVD, nr. 22a, 2009. See: http://www.ctivd.nl/?download=CTIVD%20rapport%2022a.pdf. On 27 March 2013, the CITVD announced a follow-up study of the 2009 report about international co-operation. See CTIVD, 27 March 2013, http://www.ctivd.nl/?Nieuws.

principle of 'quid pro quo': what you give, is what you get.[85] The reasoning is, that by giving away intelligence to foreign intelligence agencies, and getting some in return, intelligence agencies serve national security interests. There is a clear interest for intelligence agencies to increase their own levels of access to information in the private sector and to have as broad as possible legal powers. Interestingly, these practices are described in market terms, while privacy, confidentiality and information security interests of public and private actors are not at all mentioned.[86] As such, the exchange between governmental agencies in different countries seems to introduce a dynamic of its own: it is perceived as a means to establish a superior information position over other agencies.[87]

In such an environment, one can only speculate on the extent to which intelligence agencies in Europe have an interest in limiting U.S. government authorities access to cloud data. Perhaps agencies in Europe actually rely on the capacity of foreign agencies abroad to gain access to those data themselves.[88] A similar question could be asked about the possible reliance of American intelligence agencies to spy on U.S. persons with the help of European intelligence agencies, to avoid constitutional restrictions in the U.S. If no meaningful restrictions are placed on the exchange of foreign intelligence between agencies, it is likely that access will take place where the standards for access are the lowest. Such practices would seriously endanger information security and confidentiality interests of cloud customers in general and could endanger the trust in the market for cloud services. Regarding the probability of data access, this dynamic may cause a race to the bottom in terms of information security and data confidentiality interests.

2.2.4. Risk Assessment and Market Responses

What picture emerges from our assessment of the impact and probability of transnational intelligence surveillance of cloud data? While it is clear that cloud customers have started to seek more answers about the risks of data requests by foreign governments, it is also clear that risks can only be vaguely named and established. Thus in practice, the risk of governmental data requests for intelligence purposes will become one concern in a long list of more quantifiable risks related to information security, and be weighed against the benefits of processing and storage for commodity pricing. Such more tangible risks relate to the availability of data, data leaks, and whether cloud providers actually remove data upon deletion by the customer. In these circumstances, it is likely that more tangible risks and benefits get prioritized by low-end or even mid-end security customers. Nonetheless, none of the cloud customers will ever know what happens to their data, who has access to it and how often. This asymmetry in the information position is a serious risk and stands in the way of careful decision-making about the use of cloud services, even if governmental access to cloud data abroad is not a core concern. The risk may be structural risk, since it is not in the interest

[85] *Supra* note 84, p.12. See also Hans Born and Ian Leigh, 'Making Intelligence Accountable: Legal Standards and Best Practice', Oslo: Publishing House of the Parliament of Norway, p. 64.

[86] *Supra* note 84, p. 12,16. The risk of giving away too much information and in doing so limiting the ability of the Dutch intelligence agency for future intelligence sharing, is also recognized. According to the CITVD, Dutch intelligence analysts are driven by short term 'ad hoc' access to foreign intelligence, rather than longer term interests to national security.

[87] This mirrors what Swire has described as an increasing dependency of agencies that have no access to cloud data ('the have-nots') on those that have ('the haves'). Swire 2012 (supra note 74), p. 1.

[88] The Echelon program has been seen by many as a way to circumvent national constitutional restrictions. For a discussion, see Report on the Existence of a Global System for the Interception of Private and Commercial Communications, Eur. Parl. Doc. COM A5-0264/2001, available at http://www.fas.org/irp/program/process/rapport_ echelon_en.pdf.

of cloud providers to remove this asymmetry. Cloud providers may not even be in a position to provide an answer in good faith on these complex issues, let alone any guarantees.[89]

These developments affect market conditions and competition, impacting American cloud services in particular in the European context. Cloud providers are currently calling on regulators to provide clarity on the issue, and justifiably so. On the cloud customer side, the situation has led to calls for regulatory action and termination of cloud contracts. The next section explores several suggested legal solutions on how to address governmental access to cloud data from abroad.

3. Towards Addressing Governmental Access Abroad

A range of European policy makers have expressed their unease about the possibility of access to cloud data in the United States (and abroad more generally). Especially, the idea that United States law permits access to data about Europeans in a way that overrules European privacy and data protection standards has been both hard to swallow and understand for Europeans. European Commissioner Reding, responsible for the proposals on data protection currently discussed in the European Parliament has consistently called for respect for privacy and data protection on the U.S.-side of the Atlantic:

> "we are also counting on others to take data protection seriously. We also need others to build trust – both in the commercial and law enforcement fields."[90]

When the possibility of access in the United States under FISA was put forward in relation to biometric passport data in the Netherlands the reaction was that such access should be prevented. A Member of Dutch parliament for instance stated in reaction:

> "It is incomprehensible that one's passport data are accessible to American authorities. […] This administration is not doing enough to protect the privacy of Dutch citizens."[91]

Ms Schippers, the Dutch Minister of Health, Welfare and Sports, perhaps had the most telling reaction. In November 2012, the news broke that the Dutch patient record system was accessible to U.S. authorities under FISA as a result of the company that had been chosen to manage these data. She responded that this was "impossible", since there was a professional duty to keep such data secret in the Netherlands.[92] In other words, the protection of such sensitive data from access abroad is assumed at the highest levels of government, even though it is actually absent.

While the political will may be present in European countries to increase protection from access abroad, it is also clear that regulatory solutions will not be straightforward. Nonetheless, several

[89] This is the case in particular for cloud providers that offer software as a service and use the infrastructure of third parties for the storage and processing of cloud data; so-called SaaS providers (Software as a Service), as opposed to IaaS (Infrastructure as a Service).

[90] See Viviane Reding, 'The future of data protection and transatlantic cooperation' Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels, 6 December 2011, http://europa.eu/rapid/press-release_SPEECH-11-851_en.htm?locale=en.

[91] See D66, D66: houd Nederlandse vingerafdrukken uit Amerikaanse handen, 7 June 2012, http://site.d66.nl/d66nl/nieuws/20120607/d66_houd_nederlandse.

[92] NOS, 'Onrust patiëntendossier neemt toe' [Unrest Patient Record System Increasing], NOS.nl, 30 November 2012, http://nos.nl/artikel/446339-amerika-kan-mogelijk-in-epd-kijken.html.

proposals have already been made or are put on the table. This second part of the paper explores some of these solutions, subsequently taking the perspective of U.S. law, international law, European law, and Dutch law.

3.1. The US Level: Better Safeguards in FISA for Foreigners

The most direct solution for the issue of broad access to data of Europeans under FISA would be the amendment of the FISA's §1881a, through legislative action or as reaction of legal or political action in the United States. Amendments or requirements to be tried could include better safeguards, such as the requirement of proportionality and probable cause in a similar manner as required for U.S. persons. In addition, further restrictions in view of the civil liberties of non-U.S. persons could be included accompanied with a requirement of oversight by FISC on the proportionality of acquisitions of foreign intelligence abroad. For instance, a requirement could be added that foreign intelligence gathering of non-U.S. persons abroad should not be conducted solely on the basis of the expressive or political activities that would be protected under the First Amendment if they were U.S. persons.[93] As regards the protection of civil liberties of non-U.S. persons abroad, U.S. law could either apply its own constitutional standards to such persons or incorporate standards developed under international law.

While this would provide the most direct solution to the problem for Europeans that want better protections, the political feasibility of amending FISA in this manner seems minimal. Furthermore, U.S. law does not seem to provide for a proper way to legally complain about the lack of restrictions or procedural safeguards for §1881a surveillance. The latter problem can be best illustrated with a discussion of the recent judgment of the US Supreme Court about the FAA 2008. The former problem becomes apparent when looking at the political debate in the United States about the need to gain access to information about foreigners.

As mentioned above, the FAA 2008 was passed in the wake of a debate in the United States about the warrantless wiretapping of American citizens. In effect, it codified warrantless wiretapping into FISA, including some measures to safeguard the constitutional interests of Americans. The law remained controversial for its impact on privacy and civil liberties and ACLU, Amnesty, American attorneys and others filed a constitutional complaint soon after its passing. The legal theory underlying the challenge was directly based on the fact that claimants were U.S. persons and the FAA 2008 would lead to the warrantless surveillance of their communications. As the Supreme Court summarized:

> "Respondents believe that some of the people with whom they exchange foreign intelligence information are likely targets of surveillance under §1881a. Specifically, respondents claim that they communicate by telephone and e-mail with people the Government "believes or believed to be associated with terrorist organizations," "people located in geographic areas that are a special focus" of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government."[94]

[93] Compare 18 USC 1861(a)(1). For a discussion, see Kris and Wilson 2012.
[94] 568 U. S. ____ (2013).

But the Supreme Court's conservative 5-4 majority agreed with the U.S. Government that these claims were speculative. The Court dismissed a range of rather specific arguments demonstrating the likelihood that claimant's communications would be targeted and their First Amendment rights be affected through chilling effects of §1881a. In a rather Orwellian twist – since the whole design of §1881a should guarantee that individuals will never find out whether they have actually been targeted, the Court then concluded that:

> "because §1881a at most authorizes—but does not mandate or direct—the surveillance that respondents fear respondents' allegations are necessarily conjectural."[95]

The Court then continued to point out that even if the Government were gaining access to claimants communications, there was no proof that this access was based on §1881a and not on other legal means such as the executive order 12333 for spying abroad.

Furthering its strict interpretation of the standing requirement, the Court finally addressed the complaint by the carefully selected claimants in this case that if *they* would not have standing, §1881a could never be challenged. The Court answered to this concern by listing three possibilities in which §1881a surveillance could be legally challenged, namely (1) in the context of the FISC's of the U.S. Government's certifications, targeting procedures, and minimization procedures, (2) when the Government wants to use the information obtained in a judicial proceeding and it has to notify on the basis of 1881e(a) and 1806(c), or (3) by an electronic communications provider that is asked to assist in an §1881a surveillance program. Thus, in theory, even a European could find out in a U.S. Court that data about her had been obtained through §1881a. She would herself however not be able to challenge the legality of the surveillance since, as the Supreme Court acknowledges, she "might not have a viable Fourth Amendment claim".[96] The FISC's track record and legal mandate, finally, do not give any reason to believe that the other two options will result in meaningful scrutiny of §1881a's impact on the civil liberties of non-U.S. persons. There is simply no room for the FISC to take these interests into account. Even with regard to U.S. persons its review under §1881a is "narrowly circumscribed."[97]

If the U.S. legal system is not supportive of a claim against §1881a surveillance, the U.S. political landscape is at least equally dismissive of arguments that it should be put under stricter conditions in view of the privacy interests of foreigners. Here it must be kept in mind that the measure in question is part of the U.S. response to the terrorist attacks in September 2001. Seen in perspective, the mass surveillance of foreign countries through internet and cloud services under U.S. jurisdiction would be one of the less far-reaching measures taken in the 'War on Terror'. Consider for instance the increasing reliance on drone strikes and targeted killings.[98] While these are the measures that do end

[95] 568 U. S. ____ (2013). The dissenting opinion concludes otherwise: "*Several considerations, based upon the record along with commonsense inferences, convince me that there is a very high likelihood that Government, acting under the authority of §1881a, will intercept at least some of the communications just described*."

[96] *Clapper v. Amnesty* 568 U.S. ___ (2013).

[97] See FISC, *In re Proceedings Required by §702(i) of the FAA 2008*, No. Misc. 08–01, 17 August 2008, p. 3.

[98] Of course, it is likely that these operations are partly informed by foreign intelligence gathering based on FISA. For a critical discussion putting the drone killing operations in historical perspective, see Steve Coll, 'Remote Control, Our Drone Dillusion', The New Yorker, 2013, http://www.newyorker.com/arts/critics/books/2013/05/06/130506crbo_books_coll. See

up being discussed critically in the United States (often with reference to the fact that some targets were and could be American citizens), the impact of spying abroad through FISA's new power on the interests in privacy and confidentiality of foreigners is bit of a non-issue in U.S. politics. There is no one in U.S. Congress that urges electronic surveillance of foreigners to be put under stricter conditions. Even American civil liberty groups tend to use arguments that heavily rely on the interests of U.S. citizens or residents.[99]

If anything, one may expect the U.S. intelligence community to further increase its reach into the global information infrastructure using powers such as §1881a or new ones yet to be established by the U.S. legislature. The warnings against foreign cyber threats by U.S. intelligence officials are steadily increasing. And specific restrictions against the activities of companies like Huawei also reflect the awareness about the offensive possibilities in cyberspace of other nations, for instance through the penetration of foreign markets in telecommunications and ICT.[100] Ironically, while the U.S. Internet Freedom Agenda calls for unrestricted access of U.S. services to foreign markets, provisions like §1881a ensure that such access comes together with the *possibility* of mass surveillance of the respective populations.[101] This may certainly not be the goal of the State Department's focus on Internet Freedom. But until restrictions have been passed for §1881a surveillance of non-U.S. citizens in views of the civil liberties outside U.S. borders, there is room for serious criticism of the freedom that American Internet companies bring.[102]

3.2. The International Law Perspective: Sovereignty and Human Rights

Perhaps the way in which the U.S. is allowing itself to conduct surveillance of non-U.S. persons located abroad is a matter that should and could be addressed under international law. European Commissioner Viviane Reding suggested as much when she claimed that these matters should be resolved by the International Court of Justice in The Hague.[103] But how successful would an actual referral be? Which grounds are there under International law to complain about transnational intelligence gathering and the gathering of foreign intelligence from foreign territory? Below, three possible grounds for a claim against FAA 2008 type of intelligence gathering are discussed. First, that this amounts to an infringement of the principle of sovereignty. Second, that it is an infringement of international human rights obligations. And third, that it may be the case that a European country that fails to protect its citizens against transnational mass surveillance by other countries is in breach of its positive obligations under the ECHR to protect the right to private life.

---

also Stephen Griffin, 'The CIA and Drone Strikes', Balkanization, 2013, http://balkin.blogspot.nl/2013/05/the-cia-and-drone-strikes.html.

[99] See e.g., ACLU 2008 (supra note 27).

[100] See e.g. Michael S. Schmidt, Keith Bradsher, and Christine Hauser, 'U.S. Panel Cites Risks in Chinese Equipment', The New York Times, 8 October 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

[101] For a critical discussion of the Internet Freedom Agenda, see e.g. Evgeny Morozov, *The Net Delusion*, 2011. See also Evgeny Morozov, 'Freedom.gov', Foreign Policy, 2011, http://www.foreignpolicy.com/articles/2011/01/02/freedomgov.

[102] Similarly, the way in which the U.S. went after Wikileaks struck foreign commentators as a display of 'imperial arrogance and hypocrisy'. See Steven Erlanger, 'Europeans Criticize Fierce U.S. Response to Leaks', 9 December 2010, http://www.nytimes.com/2010/12/10/world/europe/10wikileaks-react.html.

[103] BBC Democracy Live, 'Data Protection Question', 15 February 2012, see [includes video]: http://news.bbc.co.uk/democracylive/hi/europe/newsid_9695000/9695923.stm.

In their study for the Global Network Initiative Brown and Korff conclude that foreign intelligence gathering of data from foreign territories should in principle be based on "Mutual Legal Assistance Treaties" (MLATs) or be an infringement of international law otherwise.

> "When law enforcement or national security agencies in one country want to obtain access to evidence in another country, they generally have to go through [MLATs] that protect the rights of all affected persons. MLATs are complex and can be cumbersome in practice. However, bypassing established MLAT processes constitutes an infringement of sovereignty."[104]

This raises the question about the application of enforcement jurisdiction, which on the basis of international law should not be exercised in the territory of another state without its consent, to the collection of data through cloud or electronic communications providers.[105] Although Brown and Korff do not discuss the application of this principle to different types of transnational and extraterritorial surveillance in detail, this reasoning seems to imply that transnational intelligence gathering as is taking place under FAA 2008, namely the extraction of data from a third country, is a form of illegal exercise of enforcement jurisdiction, since the data is residing abroad. In particular, there would be an infringement of specific international law that are aiming to protect the sovereignty with respect to the exercise of surveillance measures.

Looking at the available literature discussing the international law requirements for different forms of surveillance, however, and taking into account the specific configuration of FAA 2008 surveillance, there is some reason to believe that this specific type of transnational surveillance does not have to be characterized as enforcement jurisdiction under international law.[106] First, the gathering of intelligence and the exercise of power (with respect to cloud providers) under the FAA 2008 is actually taking place on U.S. territory and not abroad. Arguably, this would be different if an agent would install surveillance equipment in data storage facilities in a third country or when access would be obtained through the use of force and not by legal request. Second, the surveillance target(s) under FAA 2008 need to be believed to be abroad, but as to where the data resides geographically the law remains agnostic.

While there seems to be a general agreement in the literature that surveillance of foreigners abroad for law enforcement purposes needs to follow MLATs, in the context of transnational intelligence agency activities the situation becomes murky. Since the countries one would want to spy on would surely include the ones that would not enter into any MLAT, any intelligence gathering with respect to information originating from those countries would be illegal. In practice we therefore do not expect the requirement of MLATs for transnational intelligence purposes to be able to reflect reality.

We found some support for these arguments in a recent discussion of the legality of extraterritorial intelligence gathering under international law by Canadian scholar Forcese.[107] In his categorization of different geographical modes of electronic surveillance, 1881a surveillance has to be considered to be 'transnational'. In contrast to extraterritorial foreign intelligence gathering, for instance through

[104] See GNI, Digital Freedoms in International Law, Global Network Initiative, 2012.

[105] With reference to Vaughan Lowe, Chapter 10 --- Jurisdiction, Section III – The Fundamental Principles Governing Enforcement Jurisdiction, in: Malcolm Evans (Ed.), *International Law*, 1st ed., OUP, 2003, p. 351.

[106] Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection', 5 J. Nat. Sec. Law & Pol. 179 (2011).

[107] *Id*.

the infiltration and instalment of wiretapping equipment at the European premises of a telecommunications carrier, transnational surveillance by country X entails access to the data on the territory of X itself. Forcese concludes that even some forms of extraterritorial spying, i.e. government agents acting on foreign territory, are not clearly illegal under international law.[108] And the case against transnational intelligence is weaker, since it takes place on a country's own territory:

> "some transnational intelligence gathering may be simply passive, in the sense that an electronic signal originating in one state is captured in another. It is difficult to see how the interception of electronic leakage from one state from the territory of another state violates a sovereignty interest."[109]

Following this reasoning, the conclusion could be that European states should simply prevent sensitive European cloud data from ending up in the United States, or under United States FISA jurisdiction. Of course, the political and economic reality make this a unlikely avenue to explore for all but the most sensitive data processing operations.[110] As Reding states after complaining about U.S. privacy standards:

> "I am reading in the press more and more about European internet companies offering a cloud computing service which stays in Europe. Just yesterday I read about a Swedish company whose selling point is that they shelter users from the US Patriot Act and other attempts by third countries to access personal data.
>
> Well, I do encourage cloud computing centres in Europe - because we need more innovation, more research and more investment in the ICT industry. But this cannot be the only solution. We need free flow of data between our continents. And it doesn't make much sense for us to retreat from each other."[111]

Even if transnational mass surveillance would not an infringement of sovereignty of the other nations involved, a question that deserves more discussion in our view, perhaps it does infringe human rights obligations in the International Covenant on Civil and Political Rights (ICCPR), more specifically the right to private life as enshrined in Article 17 ICCPR. This raises the question about the extraterritorial reach of the ICCPR. Article 2 ICCPR provides that the obligation of a State to respect Article 17 ICCPR extends to "all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant".[112] The ICJ concluded in 2004 that

> "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[113]

Forcese's conclusion seems to be that in the case of mere intelligence gathering about foreign targets through third parties such as cloud providers, there is no such effective control present. In

[108] *Id*., p. 197-205.
[109] *Id*.
[110] In the Netherlands there have been discussions of putting restrictions in procurement procedures. See Walter van Holst & Marina Berghuijs, 'PATRIOTtisch aanbesteden', Tijdschrift Aanbestedingsrecht, 2012-4, p. 397.
[111] *Supra* note 90.
[112] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171].
[113] See Human Rights Comm., General. Comment 31, ¶10, U.N. Doc. A/59/40 (2004). See also supra note 107, fn 128 and accompanying text.

other words, the type of surveillance of non-US persons abroad conducted through the FAA 2008 would not infringe the U.S. obligations under the ICCPR.[114] This seems a rather restrictive interpretation and considering the nature of the right to privacy, it seems more reasonable to conclude that the exercise of power is present as soon as there is an interference with the said right.

Ironically, it may be the case that the best available course of action under international law would be a complaint of European citizens (or organizations affected by unrestricted mass surveillance) against their own country of citizenship or residence. Arguably, European Member States have a general obligation under Article 8 of the European Convention on Human Rights (the right to private life), to protect persons under their effective control from being subject of disproportional surveillance by third parties, including foreign government agencies. In general, the FAA 2008 and its broad scope without procedural safeguards are hard to align with the requirements of Article 8 ECHR. The vacuum cleaner collection it allows without a proportionality test is hard to reconcile with the proportionality and subsidiarity requirements of Article 8, second paragraph. Some argue that ECHR signatory states have a positive obligation to secure data from wrongful access. It is beyond the scope of this paper to further delve into the question of the requirements under the European Convention.[115]

To the extent that a European Member State has made it illegal for companies to become complicit in disproportional mass surveillance of European nationals under the FAA 2008, that positive obligation may be fulfilled. At the same time, even after a number of scandals involving PNR data and financial data, there remains debate to what extent there are legal hurdles that prevent companies from handing data on Europeans over to U.S. government agencies.[116] And the question remains if European intelligence agencies are actually aware of the surveillance taking place of their own populations from outside their borders. In other words, perhaps the solution should be found at the level of European restrictions on leakage of confidential data to companies under foreign intelligence gathering jurisdiction (discussed in the next section). Or, if this would not solve the issues at stake, perhaps the situation calls for increased oversight of transnational intelligence operations at the national and international level.

3.3. The EU perspective: Cloud Communication and Data Protection Regulation

Over the last months, governmental access to cloud data from abroad has been picking up momentum in EU policy circles. In a 21 February 2013 response to parliamentary questions raised as a consequence of the study this paper is based on,[117] the European Commission (EC) Vice-President Neelie Kroes, responsible for the Digital Agenda including cloud computing policy argues that the issue is addressed in two of the Commission's policy cycles. The first is a EC Communication in September 2012 titled 'Unleashing the Potential of Cloud Computing in Europe' which is currently

[114] Note that the U.S. made a reservation to the ICCPR as regards the possibility to invoke these rights in a U.S. Court.

[115] See also Council of Europe 2007 (supra note 63). See also G. Nardell, 'US access to Cloud data: the Human Rights Dimension', CPDP conference, 2013, http://www.39essex.com/docs/news/cpdp2013gn_23_01_13.pdf (referring to amongst ECtHR *Weber and Saravia v. Germany* (54934/00), ECtHR *Liberty v. the U.K*. (26839/05). At PLSC 2013, Judith Rauhofer's paper will further analyse the art. 8 ECHR aspects of governmental access from abroad.

[116] See also infra, Section 3.3.2.

[117] See EP, Question for written answer to the Commission, E-000186/2013, http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-000186&language=EN

reviewed by the European Parliament (EP) and the Council (the Member States). The second is the revision of the EU data protection framework, proposed by the EC in early 2012 and currently debated in the EP and the Council. In both contexts the issue of access to cloud data abroad is being discussed and amendments to prevent it have been tabled.

3.3.1 The EU's Cloud Policy and Restrictions on Governmental Access Abroad

From the EC's Communication on 'Unleashing the Potential of Cloud Computing in Europe' communication ('Cloud Communication')[118] and the policy documents of the European Cloud Partnership',[119] we learn that data access by 'law enforcement' agencies is being discussed with U.S. authorities. But as is also clear from section 2.2, law enforcement access to data is of a different nature than foreign intelligence gathering. The Cloud Communication makes no mention of intelligence gathering by non-E.U. governments as an issue of concern. This is somewhat curious, since several Members of the European Parliament ('MEPs') had raised Parliamentary questions on the extra-territorial application of the US Patriot Act already in 2011.[120]

Responding to the Cloud Communication, the European Economic and Social Committee ('EESC') does raise the issue.[121] It has advised that:

> "international regulations applicable to suppliers in other countries outside Europe are not currently appropriate for [cloud computing]; the best known example of this is the US Patriot Act"[122]

And it states that the EC should specifically address intelligence gathering under U.S. law in its policies:

> "[…] the Commission must incorporate safeguards for the use of [cloud computing] in public services and certain sensitive private sectors in this "Cloud First Policy" in order to control, or even prevent, data being hosted by suppliers that are subject to risky national regulations – such as the Patriot Act." [123]

The Cloud Communication is now sent to the EP and Council for a formal response,[124] and by the end of 2013 the EC will "report on the progress on the full set of actions in this [cloud] Strategy and present further policy and legislative proposals initiatives as needed."[125] It is feasible that this aspect of the Cloud Communication will be further discussed in the near future and there is enough reason to do so. Consider for instance the European Cloud Partnership's Steering Group calling for "the

[118] EC, Unleashing the Potential of Cloud Computing in Europe, Brussels, COM(2012) 529 Final, p.15.

[119] Set up in November 2012, see EC, European Cloud Partnership, https://ec.europa.eu/digital-agenda/en/european-cloud-partnership. See also EC, Digital Agenda: Tech CEOs and leaders kickstart new EU cloud computing board, 19 November 2011, http://europa.eu/rapid/press-release_IP-12-1225_en.htm.

[120] See for example EP, Questions for written answer to the Commission, E-006901/2011, E-004810/2012.

[121] The EESC is an official EU body that "contributes to strengthening the democratic legitimacy and effectiveness of the European Union by enabling civil society organisations from the Member States to express their views at European level." See EESC, 'About the Committee', http://www.eesc.europa.eu/?i=portal.en.about-the-committee.

[122] See EESC, 'Towards an EU Cloud Computing Strategy', EESC/2012/1701, TEN/494, http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=en&docnr=1701&year=2012

[123] *Id*.

[124] A plenary debate in the European Parliament on the Cloud Communication is scheduled for 18 November 2013, dossier number: 2013/2063(INI).

[125] See *supra* note 119, p.16.

migration of public IT use to the cloud" and to "move cloud use into mission critical areas of business and public life, in areas such as eID, smart cities, eHealth, eEducation, research and digital content services".[126] These include critical data infrastructure (eID, for instance, stands for the ICT infrastructure for electronic identity in Europe) for which the unchecked access by foreign intelligence agencies without well-informed policy is problematic.

3.3.2. The EC Proposed Data Protection Regulation

The ongoing EU data protection revision is seen by many as the proper instrument to ensure that foreign governmental access to cloud data meets EU standards of privacy and information security and therefore poised to influence the EU cloud policy substantially. After the EC launched its proposal in January 2012, a whopping 4373 amendments have been tabled in the EP. In the coming months – or perhaps years – the EP and the Council will debate the proposals in an ordinary legislative EU co-decision procedure. About one hundred of these amendments address governmental access to cloud data from abroad, a large number that hardly surprises, given MEPs parliamentary questions and concerns expressed in the media.[127]

In the remainder of this section, we will first point at the inherent weaknesses of data protection law as a solution to addressing governmental access to cloud data from abroad, then outline the proposed regime of third (non-EU) country data transfers by the European Commission and finally discuss relevant amendments in more detail. So far, the Council hasn't officially commented on the third country transfer provisions of the European Commission proposal.[128]

EU data protection law has some inherent limitations as a solution for governmental access to cloud data from abroad. The most obvious drawback is that only a (small) subset of cloud data constitute 'personal data'. Other cloud data for which there is a confidentiality or related information security interest – corporate and state secrets, intellectual property and other documents – are as such not covered. The definition of 'personal data' is one of the most fiercely debated aspects of the EU data protection framework. A limitation of the definition of 'personal data' – for example, whether or not pseudonymized data will be excluded – would further marginalize the use of the data protection as a regulatory solution.

A second inherent drawback is that the Regulation in art. 2(2a) of the current proposal excludes national security regulations from its material scope, similarly as the current Data Protection Directive (95/46/EC).[129] Consequently, the Regulation does not affect intelligence agency data gathering and processing, or the exchange with other intelligence services on a 'quid pro quo' basis as described in section 2.2.

---

[126] See Steering Board of the European Cloud Partnership, Public Statement, 2012, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1580.

[127] See e.g. Zack Whittacker, 'Patriot Act can 'obtain' data in Europe, researchers say', CBS News, 4 December 2012, http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/.

[128] The Council does support the clarification of the (extraterritorial) application of the data protection regime to controllers not established in the Union, but offering goods or service to data subjects within the Union. See Council, 'Specific Issues', 24 Apr. 2013, 8825/13 Dapix 74, 16529/12 Dapix 146, p. 9, 16, 19.

[129] This is rooted in art. 4(2) of the Treaty on the Functioning of the European Union, which states that national security is to be a competence for EU member states in the foreseeable future.

While data protection will not be an effective legal avenue to address such data processing practices by intelligence agencies, they are within the scope of the European framework for privacy protection, most notably the EU Charter ('Charter') and the European Convention ('ECHR'), and also the CoE's data privacy Treaty from 1981. These instruments are part of the fabric of both CoE, E.U. and member state level rulemaking. This is by no means a guarantee that all legislation actually respects such laws, but intelligence laws can and have been challenged before European courts. Several aspects of the data collection practices allowed under FISAA are problematic under the ECHR.[130]

The EC´s proposals for a General Data Protection Regulation (GDPR) contain several provisions that affect transnational data processing in the context of cloud computing.[131] These provisions build on the existing rules for transfer to third countries and the restrictions on transfers to countries with inadequate protection. The EC´s explanatory Communication states:

> "In today's globalised world, personal data is being transferred across an increasing number of virtual and geographical borders and stored on servers in multiple countries. More companies are offering cloud computing services, which allow customers to access and store data on remote servers. These factors call for an improvement in current mechanisms for transferring data to third countries."[132]

The rules on data transfers to third countries can be found in chapter V, i.e. articles 40-44 of the proposal. The proposed Articles 44(1)(d), 44(5) and recital 90 stipulate that in case of extra-territorial application of laws, such transfers may take place on the condition that 'important ground of public interest' as 'recognised in Union law or the law of the Member State to which the controller is subject' are met. Cloud providers are to assess themselves whether this is the case or not, while the EC would be able to further specify this procedure on the basis of art. 44(7).

In comparison with the existing Data Protection Directive, the derogations are more broadly formulated.[133] What exactly these new 'important grounds of public interest' entail is (not extensively) defined in recital 87 and in the explanatory memorandum: competition, social security and fisheries management are mentioned.[134] Regardless of the important question whether the new proposals actually imply a lowering of data protection standards, national security of EU member states is explicitly recognized under Union law and ECtHR jurisprudence as a 'legitimate aim' to justify an interference with the right to privacy or data protection (along with other criteria). The furthering of U.S. foreign affairs interests as mentioned in 50 U.S.C. 1801(e) is possibly not.

---

[130] See section 3.2.

[131] See EC, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), Brussels, 25 January 2012. Interestingly, the a widely leaked version of November 2011 were more strict, See EC, Proposal for a General Data Protection Regulation, Version 56, 29 November 2011 (Leaked Draft), http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf. These proposals have apparently been withdrawn before the definitive version of the Commission proposals, but were reintroduced by MEPs Weidenholzer en Albrecht.

[132] EC, 'Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century', COM/2012/09 final, Brussels, 25 January 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT.

[133] A useful reference is a EU Council document dated 30 January 2013 comparing the 1995 Directive and the Commission proposal, http://www.statewatch.org/news/2013/jan/Table%20eu-dp-reg-chart-1995-comparison.pdf.

[134] Supra note 132 p. 11-12.

3.3.3. The EP Amendments on Data Transfer in the General Data Protection Regulation

The EP amendments reflect doubt about these open-ended derogations that need to be interpreted by cloud providers on the one hand and the ability of the EC to address the issue in a delegated act on the other hand. Generally, the proposed amendments that are aimed to provide better protection against transfers without safeguards can be grouped in two. First, the amendments suggested by rapporteur Albrecht and MEP Weidenholzer, aiming to reintroduce the regulatory proposals of a leaked Commission proposal of November 2011. Second, MEP and LIBE vice-chair In 't Veld has introduced a stricter regime of her own.

The amendments proposing a new Article 43a (MEP Albrecht, Greens) on 'transfers not authorized by Union law' or a new Article 44a (MEP Weidenholzer, S&D) on 'disclosures not authorized by Union law' are explicitly aimed at access requests by public authorities or courts in third countries. [135] In essence, these amendments are quite similar.[136] First, the proposals mandate that governmental access to cloud data from abroad is based on a legal instrument. Second, these proposals would mandate cloud providers to notify data subjects of actual data requests by a public authority in a third country. This raises serious compliance problems for cloud providers that need to comply with U.S. law demanding secrecy in case of a FISA request. Some authors rightfully refer to this situation for businesses as a catch 22.[137] Third, these proposals transfer the assessment of requests from cloud providers and the EC to Data Protection Authorities (DPAs). DPAs are to assess whether there is a legal basis for the transfer/disclosure and whether important grounds of public interest are met (referring to art. 44(1d). Several critical remarks can be made of such an approach. For one, since the legality of cloud data requests still revolves around open-ended derogations, the legal barrier for access remains low. In a practical sense, DPAs have shied away to point at the problems of foreign intelligence surveillance in the past.[138]

[135] See Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the Data Protection Regulation, Rapporteur: Jan Philipp Albrecht, 2012/0011(COD), 16 January 2013, http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-501.927&format=PDF&language=EN&secondRef=04. See also Weidenholzer, Amendments 1-101, 27 February 2013, http://www.weidenholzer.eu/wp-content/uploads/2013/02/Amendments_Weidenholzer_short.pdf.

[136] According to the first paragraph of these new articles, such transfers/disclosures shall only be recognized or enforceable on the basis of a mutual assistance treaty or an international agreement between the third country and the EU or a member state. Moreover, once personal data is requested with a controller or processor, paragraph 2 mandates that he shall notify a competent supervisory authority and obtain prior authorization for the transfer/disclosure. MEP Weidenholzer makes explicit that the processor/controller must notify and obtain prior authorization. According to paragraphs 3 and 4, the supervisory authority will then assess compliance with the Regulation, particularly whether 'important grounds of public interest' are met, and notify the competent national authority (the DPA of the data subject), while the provider has to notify the data subject. The Commission may no longer formulate delegated acts on substance (for instance, what constitutes 'public interest'), while it may adopt implementing acts with regard to the procedures of notification according to paragraph 5. The Article 29 Data Protection Working Party has advised the policy community to base cloud transfers to third countries on a legal instrument in WP196, 'Opinion on Cloud Computing', 5/2012, p.23.

[137] See e.g. M.B. Voulon, 'Catch 22: Amerikaanse vorderingen tot het verstrekken van gegevens versus het aanbod op doorgifte aan derde landen', Privacy & Informatie, 2012-5.

[138] This is not that surprising since it is outside of their scope of activities to consider intelligence data processing. Confronted with a case of government mandated biometric passport data storage by a cloud provider falling under U.S. jurisdiction, the Dutch DPA responded that cloud customers themselves are responsible for making the right choice of cloud

3.3.4. The In 't Veld Amendments on Transfers to Clouds Under 3rd-Country Jurisdiction

MEP In 't Veld (ALDE and vice-chair LIBE committee) is responsible for another set of amendments that aim to address intelligence data processing from abroad. Her proposal entails stricter derogations for third country transfers in Article 44 and a special regime for 'transfers to cloud services under third country jurisdiction' in a new Art. 44a:

> **Art. 44a: 'Transfers to cloud services under third country jurisdiction'**
>
> The transfer of personal data to cloud services under the jurisdiction of a third country shall be prohibited, unless:
>
> (a) one of the legal grounds for transfer of personal data to third countries listed in this Chapter is applied; and
>
> (b) the data subject has given consent; and
>
> (c) the consent has been given by the data subject after having been informed in clear, unambiguous and warning language through a separate and prominently visible reference to:
>
> - the possibility of the personal data being subject to intelligence gathering or surveillance by third-country authorities; and
>
> - the risk that the protection of personal data and fundamental rights provided by Union and Member State law cannot be guaranteed, despite the legal basis of the transfer.[139]

The In 't Veld proposals raise several interesting angles for further discussion. We will subsequently look at the proposed regime, the compliance catch 22 for providers and proposed additional measures that aim to create legal certainty.

First, the actual objective of this regime is to raise awareness that foreign intelligence data requests may be happening and to remove open-ended legal backdoors for such practices (such as the derogation 'important grounds of public interests'), and to limit possibilities of structural intelligence surveillance on a massive scale rather than prohibiting data access outright or placing substantive burdens on the industry.[140] The value of this proposal lies in the fact that foreign intelligence surveillance is brought to light, rather than being hidden in the micro-politics of contractual agreements between cloud providers and customers. Thus, the proposals respond rather well to the risks of information asymmetry identified in section 2. High-risk security customers will find that this approach assists them in risk- and cost-benefit analyses. Recent rather uninformed discussions in The

provider. See NOS, 'CBP: risico's aan gebruik cloud', 13 October 2012, http://nos.nl/artikel/429075-cbp-risicos-aan-gebruik-cloud.html

[139] See EP, LIBE, Amendments amendment #2531, http://www.europarl.europa.eu/committees/en/libe/amendments.html.

[140] The proposed new regime prohibits data transfer to third countries, unless the legal grounds of chapter V of the GDPR are met. An adequacy decision (Art. 41), mutual legal assistance treaties or other international agreement (Art. 42), a binding corporate rule Art. 43) or a derogation (Art. 44) must be in place. The 'important public grounds' exception and the authority for the EC to adopt delegated acts are deleted entirely from Art. 44 on 'derogations'. And a sentence is added to the body text of the same Art. 44 on derogations, that derogations cannot be deemed legal 'to the extent it [data processing] is not massive, repetitive and structural'. Systematic mass surveillance from abroad seems explicitly prohibited under this regime. In addition, the new Art. 44a deems that cloud providers have an obligation to notify data subject about the possibility of foreign intelligence access requests when signing into a their cloud services.

Netherlands around the risks of cloud storage of sensitive data could have been prevented. Or the implications of access abroad could at least have been taken into account in an earlier phase of decision making.

The catch 22 for cloud provider compliance described before is taken away on one level, but further complicated on another. With regard to the problematic notification by cloud providers of data subjects and DPAs of individual requests, as suggested by the MEP Albrecht/Weidenholzer, only a general notification requirements about the possibility of such surveillance has to be made. Cloud providers are enabled to comply with secrecy obligations under U.S. But in prohibiting systemic surveillance on a massive scale, declaring the supremacy of EU law and demanding that legal disputes about third country surveillance should be settled before the EU courts,[141] the cloud compliance catch 22 is further complicated. While the protection against the extra-territorial application of U.S. laws has been regulated by the E.U. before,[142] U.S. intelligence (and law enforcement) requests will keep on coming, and the situation persists that cloud providers will be either in breach of U.S. or E.U. law.

The In 't Veld proposals also introduce additional measures to create legal certainty with regard to foreign intelligence data processing and its possible conflicts with EU laws.[143] These proposals could be very valuable on the long run. As mentioned before, in its Cloud policy discussed above the EC is conducting a dialogue with the U.S. on law enforcement,[144] but these amendments create an explicit obligation for the EC and European Data Protection Board ('EDPD') to address jurisdictional conflicts in light of foreign intelligence and privacy protection.

This discussion shows that governmental access to data from abroad is being addressed at the EU policy level in two different contexts but it remains questionable to what extent this will lead to a meaningful regulatory answer to the risks of governmental access to cloud data abroad. Most of the attention is directed at the Regulation, perhaps due to a whole tradition of data protection mediating privacy in transatlantic relations. But this approach has its limits, since the issue extends beyond the confidentiality of 'personal data'. Perhaps it would be better to address these issues within the recently initiated policy for cloud computing. Having said that, it may still take years for these proposals to materialize. Nevertheless, they could further initiate the need or de facto obligation to move data from non-compliant systems to compliant systems. This would have a significant economic impact on the cloud industry.

[141] In recital 90 and a new Art. 42a(3a).

[142] See Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country. Official Journal L 309 , 29/11/1996, p. 0001 – 0006, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML.

[143] The Commission has to 'clarify and resolve jurisdictional conflicts with third countries' (In amendment #2534, introducing a new Art. 45(1d-a) and a new Art. 71a is proposed in which 'the European Data Protection Board shall have a legal service' (paragraph 1) that has clarifying jurisdictional conflicts with third countries' as one of its explicit responsibilities (paragraph 3d).

[144] See supra note 119, p.15 (naming some of the fora: "the EU-US Information Society Dialogue, the European America Business Council and the EU-Japan Information Society Dialogue. Cloud may also be considered by the Transatlantic Economic Council and the EU-US SME Cooperation.").

3.4. Improving Oversight over Transnational Intelligence Gathering in the Netherlands

A final and in the view of the authors probably preferable way of addressing the issue of governmental access to cloud data from abroad by is to look at the way in which oversight over intelligence agencies could take account of these practices. This may require increased focus on international cooperation in national systems of oversight, the strengthening of transparency about such practices and the investigation into the rise and risks of transnational spying in the networked information environment brought forth by cloud computing and the global internet. Although this may not be the most easy path to address governmental access from abroad, in the end it may be the most sensible one.

Oversight over intelligence agencies, even if restricted to the national context, is inherently complicated and somewhat limited.[145] Simply put, the transparency on part of the intelligence operations that oversight requires is difficult to realize given the cloak of secrecy under which intelligence agencies operate. This was nicely described a recent scientific study about the organization of oversight on intelligence agencies in the Netherlands commissioned by the CTIVD, the official Dutch Review Committee on the Intelligence and Security Services.[146] In the study, Cyrille Fijnaut, a international and comparative criminal law scholar, comes to one clear conclusion. No one has a simple solution to the problem of balancing the effectiveness of intelligence agency operations (partly dependent on secrecy) and the effectiveness of control and oversight (partly based on transparency). If one wants to balance the interests of all stakeholders involved one naturally ends up with a very complex system.[147] The study recommends a continuous and vigilant interaction of stakeholders to give meaning to ('in the spirit of') the legal provisions on oversight.[148] If deliberation and confrontation is absent, checks and balances run adrift. The study explicitly warns that stakeholders tend to take over assigned roles and functions of other stakeholders if the needed interaction is lacking.

The study does not specifically address the complexity of proper oversight over transnational intelligence gathering, although at this level of interaction about transnational intelligence gathering much progress could be made.[149] The responses of both the EC and the Dutch government on parliamentary questions are telling. State Secretary Teeven reassured the parliament that upon bringing the issue up with their U.S. counterparts, the American authorities had "assured him" that when data are physically located in the EU, they always go through mutual legal assistance

[145] For a discussion, see Review Committee on the Intelligence and Security Services (ed.), Accountability of Intelligence and Security Agencies and Human Rights, Proceedings of International symposium 7 and 8 June 2007 The Hague, The Netherlands, 2007.

[146] C. Fijnaut, 'Wiv 2002-2012: Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel', CTIVD 2012, p. 101, http://www.ctivd.nl/?download=Boek%20Cyrille%20Fijnaut%20Wiv%202002-2012.pdf. The occasion for this study was the 10-year anniversary of the Dutch (modernized) law on the intelligence agencies (Wiv 2002) and therefor the 10-year anniversary of the oversight agency CTIVD.

[147] *Id*., p. 101.

[148] *Id*., p. 101-102.

[149] See also Bignami, 'Towards a Right to Privacy in Transnational Intelligence Networks', 28 Mich. J. of Int. L. 663 (2007).

procedures to gather these data."[150] This is simply not true, not even in the law enforcement context (that U.S. authorities always go through MLATs), let alone a requirement for foreign intelligence gathering under FISA. In fact, the responses systematically neglect the particularities of intelligence gathering (while focusing on law enforcement), even though the questions explicitly ask for their views on those particular schemes.[151] This is hardly the kind of interaction and confrontation the study about intelligence agency oversight mentioned above must have had in mind.

In some way, transnational access to data is the opposite of international intelligence data sharing between agencies. Clearly, from the geo-political perspective of the Netherlands, co-operation with the U.S. is paramount. This leads to the question how international cooperation with foreign intelligence agencies is legally organized in the Netherlands and to what extent transnational intelligence gathering plays a role in that organization.

Like FISA, the Dutch Intelligence and Security Services Act 2002 (Wiv 2002) contains various provisions regulating the gathering of data. It may be worth noting here that in comparison with the United States, the safeguards are often lower than those applicable under FISA *for U.S. persons*. Under Section 59 of the Wiv 2002, it is possible for Dutch intelligence agencies to supply data voluntarily to their foreign counterparts. And it makes it legal and possible for the agencies to provide assistance at the request of agencies of other nations. Such assistance may involve the exercise of special powers such as wiretapping and data access requests to Dutch organizations or businesses.[152] When asked to use special powers, such as wiretapping for foreign agencies, the Dutch agency should independently assess whether the exercise of the powers is consistent with the Dutch law and constitutional safeguards, which includes Article 8 ECHR. When the CTIVD recently looked into the compliance in the context of international SIGINT assistance, it found that such assessments were not always made properly.[153] If the Dutch intelligence agency is on the receiving end of the information exchange, there are less legal conditions. The general rule for cooperation including data sharing is then applicable. In principle, no cooperation should take place if it would be against the interests pursued by the Dutch agency. The respect for human rights and the sovereignty of the Netherlands are criteria that are part of this determination, but the CITVD also notes that these criteria have been loosely applied in recent years.[154]

The Dutch oversight framework could be used to further uncover the scope of transnational surveillance from abroad and the subsequent risks for Dutch society. The legal basis for data sharing by Dutch intelligence agencies in combination with the availability of lawful mass surveillance capabilities of Europeans under FISA in the US, presents a clear danger that safeguards for

[150] *Dutch Parliamentary Papers II*, 2012-13, nr. 359774, 13 March 2013, p. 2, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/03/16/antwoorden-kamervragen-over-dat-de-vs-mogelijkheden-heeft-om-in-clouddata-te-graaien.html .

[151] *Id*., p. 3. We do not mean to imply that the expanded use, application and enforcement of MLATs in the context of transnational data requests for law enforcement or other purposes should not be promoted at the national and international level. See also *supra* note 104.

[152] Notably, foreign agencies are not allowed to operate on Dutch territory independently.

[153] CTIVD, 'Toezichtsrapportage inzake de inzet van SIGINT door de MIVD', CTIVD nr. 28, 23 August 2011, pp. 59-60. The wording of this study could suggest that such independent assessment is (almost) never made.

[154] CITVD, 'De samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten', CTIVD, nr. 22a, 2009, p.ii. See: http://www.ctivd.nl/?download=CTIVD%20rapport%2022a.pdf.

intelligence gathering of foreign population are circumvented through international cooperation.[155] Considering the lack of safeguards for non-U.S. persons located abroad under U.S. law, the U.S. could, in theory, become a safe haven for mass surveillance and data mining about Europeans.

If the CTIVD would try to research this issue - the extent to which transnational surveillance is taking place and to what extent the Dutch agencies are complicit in it - it would probably face some hard obstacles that could only be overcome by working together with other oversight agencies at the international level. First, it is unlikely that information coming from agencies is officially marked as being obtained through transnational surveillance.[156] Generally speaking, agencies do not tend to disclose their techniques in the context of information exchange.[157] The use of transnational methods undermines the negotiation position of agencies, since they no longer have privileged access to data about their own citizens. There are strong incentives for the agencies not to inquire under what conditions information is obtained by other countries, since this could only lead to less access and embarrassment, for instance that information has been obtained through the use of torture.[158] Finally, it may be so that "information is supplied on terms that the source is not revealed to any other body, including the courts or whatever the oversight bodies exist in the receiving State."[159] This would complicate matters considerably.

In April 2013, the CTIVD has announced that it will further investigate the international cooperation between agencies and in particular the dependence on such foreign intelligence agencies. In this context, the question of whether the Dutch intelligence community ends up profiting from the transnational surveillance of the Dutch population could be addressed as well. In addition, the Dutch intelligence agency AIVD has announced that it is actively looking into the threat of access to data from abroad by foreign governments or non-state actors. The agency will support measures to protect information the confidentiality of which is necessary for national security, also in view of the possibility of access by state actors abroad.[160] In this context, it will advise the Dutch government about preventive measures (in terms of safe products and architecture) and detection and response." This suggests that the Dutch intelligence agencies will in fact be looking into the issue of cloud access from abroad in contexts such as the Dutch Ministry of Defense. While those institutions may not be interested in protecting Dutch journalists or activist groups from wholesale access to their data under the FAA 2008, they do end up dealing with the same systemic vulnerability.

4. Conclusion

Foreign data access is obscured by the cloud, with serious consequences for decision-making about cloud providers in the market, especially from the perspective of medium and high security

[155] The same is of course true for the new proposed powers for the Dutch Intelligence community to wholesale wiretap cable based communications in the Netherlands (and the possibility that this information, including information about U.S. persons) is handed over to the United States.

[156] For a discussion, see nr. 117, http://www.statewatch.org/news/2007/jun/venice-com-control-of-security-services.pdf.

[157] Supra note 84, p. 9. (Quoting the Minister of Internal Affairs saying "Intelligence and security services also keep their methods secret in their collaboration with each other").

[158] See Council of Europe 2007 (*supra* note 63), nr. 118-119.

[159] *Id*., nr. 120.

[160] Dutch General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD), https://www.aivd.nl/@2988/jaarverslag-2012/.

demanding cloud customers. The discussions in Europe about the PATRIOT ACT and other U.S. laws (FAA 2008) that could grant access without meaningful restrictions illustrates the complexity of the issue at the legal and policy level. This Article has addressed the existence and risks of transnational intelligence gathering in the cloud context and the appropriate legal responses to it.

After a period of shying away from the issue, the governmental access to data from abroad is now being addressed at the EU and national level. And although popular discussions remain somewhat ill-informed, a more nuanced discussion of the issues is starting to emerge. Most of the attention is directed at possible amendment of the data protection framework, but this has inherent limitations, particularly the fact that only a small portion of cloud data actually constitutes personal data within the definition of the Data Protection Directive, and the currently negotiated Regulation appears to further limit that definition. It would make more sense to address these issues within the Cloud Communication, to the extent that this is possible under the EU Treaty. Of all the suggested proposals, the In 't Veld amendments about data transfers and cloud computing are the most ambitious. They would introduce an interesting new transparency obligations towards cloud customers and restrictions on bulk access such as the acquisitions made possible by the FAA 2008 in the U.S.

We conclude that the international law perspective on the matter of transnational surveillance deserves further attention but may be more nuanced than that it is in and by itself an infringement of international human rights and national sovereignty. Transnational surveillance has an impact onm foreign territory but the requests for access take place on the territory of the country claiming transnational intelligence jurisdiction. While the intrusion of law enforcement or intelligence agencies into computers on foreign territory does entail the extraterritorial use of power, transnational surveillance through internationally operating cloud or communications services may not be an infringement of international law. The international human rights framework and the ECHR could be valuable in the relation of citizens with their own government that would fail to protect critical personal data infrastructure from governmental access abroad.

Not the easiest, but probably the most sensible way to address the issue, however, would be through the application and possible strengthening of oversight over intelligence agency operations. Strengthening oversight could start at the national level through application of existing legal powers. In the Netherlands, the CTIVD could address this in its planned investigations about international cooperation and dependence on foreign agencies. In addition, the possibility of transnational surveillance could be addressed by the legislature, for instance by requiring that the Dutch agencies should not be able to profit from information obtained about Dutch citizens from abroad without appropriate safeguards. In all of this, it should also be kept in mind that national intelligence agencies themselves have very good reasons to be worried about and investigate the possibility of access by foreign governments abroad. Considering all the interests involved in the transition to the cloud, it will be hard but must be possible to come to some agreement about restrictions on transnational intelligence gathering.