Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act

Dr. J.V.J. van Hoboken, A.M. Arnbak, LL.M. & Prof. Dr. N.A.N.M. van Eijk,

with the assistance of N.P.H. Kruijsen, LL.M.

Institute for Information Law

University of Amsterdam

http://www.ivir.nl

November 2012 (English Translation)

Version 1.1 (Footnote 29 and reference added)

Institute for Information Law

Faculty of Law

University of Amsterdam

Kloveniersburgwal 48

1012CX Amsterdam

The Netherlands

http://www.ivir.nl

Translation of J.V.J. van Hoboken et al., Cloud diensten in Hoger Onderwijs en Onderzoek en de USA Patriot Act, Instituut voor Informatierecht in opdracht van SURFDirect, September 2012.

Management summary

The transition to cloud computing raises a host of questions. A recurring question is whether this transition has implications for access to data by foreign governments. In this context, mention is often made of the U.S. government and the Patriot Act, which would permit authorities in the United States to request data stored on behalf of Dutch cloud service users. This study, commissioned by SURFdirect[1], examines the extent to which this is actually the case, seen from the perspective of higher education and research institutions in the Netherlands. The study also addresses the question how best to manage this risk.

The USA Patriot Act has come to play a symbolic role in this debate. In addition to addressing this specific law, enacted in 2001, this report looks into the wider legal framework in the United States and the Netherlands governing access to data for law enforcement and national security purposes. The report then places the legal risks identified in a broader perspective by examining information confidentiality and security in general. Based on this analysis, recommendations are made for informed decision-making in the higher education and research sector.

The answer to the question concerning the possibility of accessing data stored in the cloud by the judicial authorities and intelligence agencies in the United States is both straightforward and complex. Under U.S. and Dutch law, the police, the judiciary and intelligence agencies are able in one way or another to request information from higher education and research institutions and any other parties concerned. The transition to cloud computing has not, in principle, changed this situation. When using a cloud service provider that is subject to U.S. jurisdiction, data may be requested directly from the company in question in the United States. If no such jurisdiction applies, data may be retrieved either with the assistance of the Dutch judicial authorities or intelligence agencies, or from a cloud service provider or the institution itself. From a legal point of view, access to such information cannot be denied and cloud service providers can give no guarantees in this respect.

Having said that, the powers available to the U.S. authorities to access data vary. In the case of data that can be requested directly from the cloud provider, for example, U.S. law offers Dutch cloud users very little legal protection; under Dutch law, however, legal protection *is* offered for requests of this kind. Guarantees provided by the U.S. Constitution in the event of U.S.

[1] SURFdirect is part of SURF, the Dutch umbrella organization for ICT-driven innovations in higher education and research.

government requests for information do not apply to Dutch users of the cloud. And legal protection under specific U.S. laws applies primarily to U.S. citizens and residents.

The relevant U.S. legislation offers ample opportunities to request data stored in the cloud. In the case of intelligence agencies, there are few substantive barriers in this regard. Note that these powers are not only provided for under the 2001 Patriot Act, but are rooted in a complex and dynamic system of powers the U.S. government has in the realm of criminal investigations and national security. Given the nature of intelligence work, it is not possible to gain insight into actual requests for information by the U.S. authorities, other than a description of the general legal framework. Cloud providers will typically not be able to disclose whether such requests are made. Yet requests by governments to access data stored in the cloud are expected to increase in the future. From a Dutch perspective, the lack of regard in the United States for the data confidentiality concerns of non-American citizens does not make matters any better. Note in this context that this issue has already been put on the agendas of the Dutch parliament, the European Parliament, the European Commission and the Article 29 Data Protection Working Party.

This report concludes that higher education and research institutions should seek to gain more insight into and keep abreast of the various forms of access to data enjoyed by judicial authorities and intelligence agencies. They should, at the same time, identify the related risks. The authors recommend that these insights be included in a general cost-benefit analysis that addresses all social and economic interests that are at stake. This includes such information management issues as information security and confidentiality, the privacy of those concerned, as well as academic freedom – a characteristic of academia – and the risk of chilling effects on those involved. It also recommends that the higher education sector make a risk analysis based on a classification of the various types of data that could be requested. It would then be advisable to develop alternatives for data that might pose an unacceptable risk if they were to come into the possession of a foreign government in a non-transparent manner.

The fact that governments have access to information is not new, of course. When making the transition to cloud computing, institutions of higher education can further build on their existing protocols and policy, as well as on the considerations they have made in the past in response to actual requests for information. It is an issue that needs to be addressed when organizations decide to engage cloud services. In doing so, they must ensure that cloud providers do not create a false sense of security. The possibility that foreign governments request information is a risk that cannot be eliminated by contractual guarantees. Nor do Dutch privacy laws offer any safeguards in this respect. The cloud provider itself should be able to convincingly answer the question whether it is subject to U.S. legislation, which often appears to be the case. It is a persistent misconception that U.S. jurisdiction does not apply if the data

are not stored on U.S. territory. The key criterion in this respect is whether the cloud provider conducts systematic business in the United States, for example because it is based there or is a subsidiary of a U.S.-based company that controls the data in question.

The transition to cloud computing will, in principle, result in a lower degree of autonomy for higher education and research institutions in terms of requests for information of the type discussed above. In this light, the specific risks run in the case of certain categories of data need to be carefully examined. This should include the question whether there are data for which a lack of autonomy would be unacceptable. The people responsible for this within the educational institutions should, moreover, realize that it is not a problem that can be solved overnight. It's an issue that should be given due consideration in the ongoing decision-making process about cloud computing in higher education and research. People at the highest levels need to provide input on possible alternatives that could offer better legal protection. The ongoing development of ideas about a national cloud could offer a solution here. The sector could also contribute to the political debate about the extensive access and jurisdiction assumed by the U.S. government. Additionally, it is important that lock-in does not stand in the way of improved decision-making based on new insights gained in this complex field.

CONTENTS

1. Introduction and research question

1.1 Cloud services and the Patriot Act

The legal implications of cloud computing have been the subject of much debate in recent years. In light of ongoing developments relating to the use of cloud services in higher education and research, the debate is also relevant to this sector. Given its key role in the academic community in the Netherlands, the Dutch umbrella organization for ICT-driven innovations in higher education and research (SURF) commissioned this study with a view to gaining a better insight into the existing legal framework. This should enable it to contribute effectively to the decision-making process about the use of cloud services by institutions of higher education and research.[2] This use of cloud computing consists of the use a wide array of services, such as email, document sharing, and contacts.[3]

An important question in the debate is whether information security and data confidentiality can continue to be guaranteed in the transition to cloud computing. What will be the implications for privacy, for the protection of personal data and for information security if the data of students, researchers and managers are no longer controlled in their own ICT environments, but end up in an electronic environment offered by a third – possibly foreign – party? Do Dutch and European privacy laws permit the storage of these data by an American provider – the major cloud service providers are U.S. based companies – outside European territory, where less strict rules apply with respect to the protection of personal data?[4] And could a situation arise in which the cloud service provider is required by a foreign government entity to disclose information in the context of criminal investigations or national security? If that is a possibility, how should it and its associated risks be assessed?

This report addresses the last two questions: what are the implications of the transition to cloud computing for access to data by foreign intelligence and law enforcement agencies, and what are the risks involved for institutions of higher education and scientific research in the Netherlands? At this point, the implications of existing U.S. legislation are uncertain and have become the topic of debate, with a particular focus on the implications of the 'USA Patriot Act'. This Act, as well as comparable statutory provisions in the United States such as the Foreign Intelligence Surveillance Act, permit authorities in the United States to request data stored on behalf of Dutch cloud service users. As a result, the Patriot Act is frequently referred to in discussions about the cloud, whether in the media, the political arena, among policy-makers in the Netherlands, or elsewhere, such as by higher education and research institutions when negotiating cloud computing contracts. In view of these discussions and the need to properly assess the risks for the privacy of end users and for the information security of the data

[2] See, for example, SURF, 'Privacy en Security in de Cloud', http://www.surfsites.nl/cloud/wat-is-cloud/privacy-en-security-in-de-cloud/. See also SURFNET 2010.

[3] This report uses the generally accepted definition of cloud computing of the NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." See NIST 2011, p.2.

[4] Research into this issue was commissioned by SURF and carried out by TILT. See TILT 2011. See also Article 29 Working Party 2012.

stored, an understanding of these legal instruments is required. This study seeks to bring clarity to this discussion, in which there is a pressing need for a proper overview of the facts and real risks.

1.2 Research question

This report addresses the implications of the Patriot Act (USA PATRIOT Act) and the risks it may pose in terms of privacy, information security and confidentiality as a result of the use of cloud services by higher education and research institutions. Given the content of the Patriot Act, it looks into the powers of government (in particular the U.S. government) to access data in the cloud in the context of criminal investigations and national security. This is not the same question as the issue referred to above regarding compliance with European and Dutch law governing personal data protection.

To be able to answer the question whether the information security and privacy of cloud service users will continue to be sufficiently guaranteed, a number of points should be borne in mind. First, we note that the Patriot Act has come to play a symbolic role in the public debate, and that in practice we are dealing with a more complex interplay of legal powers and safeguards provided for in U.S. legislation in connection with access to data for law enforcement and national security purposes. Given this complexity, a study of the implications of a particular legal instrument such as the Patriot Act should necessarily include a review of all comparable norms in the national legislation concerned. In view of the possible repercussions for the trade interests of the American businesses involved, the European concerns about access to data in the cloud by US authorities have not gone unnoticed.[5] As a result, some of the information provided in this field is somewhat biased because of the strategic importance of dispelling the concerns that have been raised.[6]

A second point is that a study into the implications mentioned above needs to address not only the implications and risks of the specific statutory framework for cloud computing, but also the extent to which these risks vary depending on the type of cloud services and the circumstances under which they are provided. Pertinent questions in this context relate to the existence of jurisdiction and the relevance of the geographical location where the data are stored. These questions feature prominently in the debate about cloud computing and the Patriot Act.[7] Are the privacy and information security risks really smaller in the case of alternatives for services provided by companies such as Google and Microsoft, if, for example, the data are stored on Dutch or European territory? What is the value of contractual guarantees in this respect? To what extent does it matter for the U.S. legal framework whether or not the provider is based in, has an office in or conducts business in the United States? And what are the advantages of a European or strictly Dutch cloud service provider for higher education and research in the Netherlands?

Third, it is important to place the risks for information security and privacy in a broader perspective. Of special importance in this regard is whether disproportionate attention is being paid to the risks arising

[5] See, for example, Rauf 2011.

[6] See, for example, Kennard 2012 and recently, Hogan Lovells 2012 (a law firm for the cloud industry).

[7] See, for example, Baker 2011; Bruins 2011, p. 48; Betlem 2012.

from the Patriot Act. Other nation states, including the Netherlands, have comparable provisions in place for access to data in the context of law enforcement and national security. And from an information security perspective, other risks and dependencies relating to cloud computing may deserve equal attention. A better insight into these risks and dependencies is needed in order to develop informed cloud computing policies that take the possibility of data retrieval by foreign governments into account.

1.3 Structure of this report

In view of the above, this report is divided into three sections, followed by a conclusion and recommendations. The first part (Section 2) describes and explains the Patriot Act and comparable relevant legislation in the United States. It also addresses the constitutional safeguards for privacy and data confidentiality in the United States (*Fourth Amendment*) and the dynamic character of the existing statutory framework, as shown by recent developments in the area of cyber security legislation. In addition, the section shortly considers the existing statutory framework in the Netherlands governing requests for data from cloud providers, and gives some examples of legislation in other European countries.

The second part (Section 3) discusses the implications for cloud service use from the Netherlands of the American statutory framework governing requests for data from cloud providers in the context of law enforcement and national security. It first assesses the powers available to U.S. authorities to gain access to cloud data of higher education and research institutions both in the context of foreign intelligence and for the purpose of criminal investigations. These powers are then placed in context by briefly comparing them with the statutory framework in Europe and the Netherlands. How this legal framework works out in practice is then illustrated with the aid of three scenarios. Each of these scenarios concerns the request for access to data from the cloud by government authorities. The scenarios include a discussion of various types of cloud services and their implications for the possibility of requests for access, as well as the possible implications for the legal protection of those concerned.

The third part of this report (Section 4) outlines how institutions of higher education and research in the Netherlands should assess, from a legal point of view, the risks arising from the existing powers granted under U.S. legislation. When answering this question, specific attention is paid to the question of how the issue can be addressed in the existing framework for the protection of data confidentiality.

1.4 Acknowledgments

The research for this report was carried out by the Institute for Information Law (IViR, University of Amsterdam, www.ivir.nl) and commissioned by SURFdirect, the SURF Digital Rights Expertise Community. SURFdirect is part of SURF, the Dutch umbrella organization for ICT-driven innovations in higher education and research. When conducting research commissioned by third parties, IViR adheres to the principle of academic integrity embraced by the Royal Netherlands Academy of Arts and Sciences,

KNAW.[8] The project was carried out by Dr. J.V.J. van Hoboken, A.M. Arnbak, LL.M. and Prof. Dr. N.A.N.M. van Eijk with the assistance of N.P.H. Kruijsen, LL.M. The research is based on a study of primary legal sources and literature.

[8] http://www.knaw.nl/content/Internet_KNAW/actueel/bestanden/wetenschappelijke_onafhankelijkheid.pdf

2. Cloud computing and data access requests from the United States: the legal framework

This section describes the U.S. legal framework for requests for access to data in the cloud. First, it describes in broad outline the American constitutional privacy safeguards in relation to government access to data (Fourth Amendment) and the doctrines developed by the United States Supreme Court concerning the protection afforded by the Fourth Amendment. It then goes on to consider the legislation that provides government authorities with powers of access, such as the Patriot Act, the Foreign Intelligence Surveillance Act (FISA), the provisions of the recent FISA Amendments Act of 2008 (FAA) and relevant provisions outside the field of the intelligence agencies such as the Electronic Communications Privacy Act (ECPA) and the recent Cyber Intelligence Sharing and Protection Bill (CISPA). Finally, it takes a broader look at the legal framework for data access requests in relation to cloud computing by briefly considering comparable legislation in European countries in general and the Netherlands in particular, and the constitutional safeguards that apply here to government access to data in the cloud.

2.1 Constitutional protection in the United States

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.[9]

In *Katz v. United States* the U.S. Supreme Court held that this protection covers situations in which a person has a 'reasonable expectation of privacy'.[10] However, this protection is limited in significant ways by what is known as the 'Third Party doctrine'.[11] The essence of this doctrine is that if one hands over one's personal 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.[12] The constitutional protection afforded by the Fourth Amendment thus ceases to apply in situations in which data are managed by third parties. The Third Party doctrine is viewed by commentators as problematic in relation to the Internet environment since the relinquishment of data is inherent in the use of the Internet. Under this doctrine, a person who relinquishes data to an electronic services provider such as an Internet Service Provider (ISP) can, in principle, no longer invoke a constitutionally guaranteed 'reasonable expectation of privacy'.[13]

[9] United States Constitution, Bill of Rights, adopted 1791.
[10] *Katz v. United States*, 389 U.S. 347, 361 (1967).
[11] *Katz v. United States*, 389 U.S. 347, 361 (1967). See also *United States v. Miller*, 425 U.S. 435, 443 (1976).
[12] See also Solove 2004, pp. 200-209.
[13] For a discussion of this matter see Kerr 2004, p. 3.

For the purposes of this study, it is also important to note that the protection afforded by the Fourth Amendment as described above can be invoked only 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*:

> 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.[14]

This means that Dutch or other foreign 'users' of American cyberspace who have no other connections with the United States are not entitled to the protection of the Fourth Amendment.[15] There has also been considerable debate in the American literature on the precise nature of this protection for U.S. citizens. However, as this protection is not, in principle, available for Europeans, this debate is basically not relevant to the present study.[16] In its decisions, the Supreme Court has indicated that comparable protection (i.e. comparable to that of the Fourth Amendment) will have to be imposed through other political channels and cannot be inferred from the U.S. Constitution:

> 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.[17]

In view of the above, the conclusion must be drawn that the Fourth Amendment plays no role of importance in relation to the question whether U.S. government entities can access data of users of cloud computing services from the Netherlands if these services come under U.S. jurisdiction.

The question of what agencies are subject to U.S. jurisdiction is answered in American 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 'activities within the borders of the United States', U.S. law applies in principle.[18] If a company has a subsidiary or branch 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.

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

[15] See Banks 2010, pp. 1656-1657.

[16] See, for example, Banks 2010, footnote 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.').

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

[18] *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984). In this case dating from 1984 the U.S. Supreme Court held that the place of data storage is not decisive: 'The foreign origin of the subpoenaed documents should not be a decisive factor. ' The principle of extraterritorial jurisdiction is also applied elsewhere, for example in Australia. See *Bank of Valletta PLC v. National Crime Authority* [1999] FCA 1099.

> 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.[19]

It follows that the location where the retrievable data are stored by a service provider is in any event not decisive for determining whether the provider in question is subject to U.S. jurisdiction and can thus be faced with the exercise of statutory powers concerning access to the data of its users.

In response to the parliamentary debate in the Netherlands on biometric data at the company Morpho, the Dutch Minister of the Interior came to a similar conclusion on the basis of an opinion of the Dutch state advocate. Data can be demanded by U.S. government authorities if the activities of the business concerned in the United States are of a continuous and systematic nature. This possibility also exists in relation to associated companies with activities in the United States if these companies possess, keep or control the data concerned.[20]

2.2 Statutory framework of lawful access provisions in the U.S. (Patriot Act, FISA, FAA, ECPA and SCA)

2.2.1 Introduction

U.S. legislation includes a series of specific provisions giving government entities powers to obtain access to data. Below is an overview of the laws and provisions most relevant from a Dutch perspective and the conditions and legal protection afforded by U.S. legislation in connection with these provisions.

The complex and extensive legislation in question provides for the exercise of coercive measures in connection with law enforcement and national security. 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 constitutional protection for the privacy and confidentiality of communication by setting statutory limits.

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), the FAA (FISA Amendments Act of 2008) and the ECPA (Electronic Communications Privacy Act).

2.2.2 The Patriot Act

The Patriot Act was enacted in 2001 in the aftermath of 9/11, and is often perceived as having created a situation in which 'data that are managed by a U.S. company can always be obtained by the U.S. authorities'.[21] This perception is a greatly simplified representation of the legal position in the United

[19] See Hogan Lovells 2012, p. 5.

[20] Dutch Lower House 2011-2012, 31 734, no. 8, p. 2.

[21] See Whittaker 2011. The Patriot Act has been described in these terms on various occasions in the Dutch parliamentary debates. See, for example, *Parliamentary Papers II* 2010/11, 3516 (Parliamentary questions raised by member of parliament

States. Rather than being an independent statute, the Patriot Act is in fact a comprehensive amendment to the then existing statutory law. In some respects it simplified pre-existing procedures for requesting data from businesses, for example Title 50 USC, Section 1861 which is discussed below.[22] However, the Patriot Act itself granted few new powers and should mainly be viewed as a framework law that amends numerous other older laws in various ways.[23] 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.[24] The most recent extension took place on 26 May 2011.[25]

The main provisions of the Patriot Act relevant to this study 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 in the interests of national security. The ECPA concerns wiretapping and 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). The latter amendment added a specific provision relating to ´Procedures for targeting certain persons outside the United States other than United States persons´.

Below is a description of the conditions on which a U.S. government entity has the statutory power to gain access to data. Analysis of how these data are then processed and exchanged and the specific government entities and officers that play a role in this connection is beyond the scope of this study. It should also be noted here that only limited information is available about 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 and the FBI and the extent to which their remits overlap. The Washington Post recently published a study of the complex interplay between the intelligence and security agencies in the United States.[26]

Elissen (PVV) about European data managed by American companies). *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 Udo de Haes 2011.

[22] For example, 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 2005, p. 59.

[23] See Kerr 2003, pp. 607-608.

[24] 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.

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

[26] See The Washington Post 2011.

2.2.3 The Foreign Intelligence Surveillance Act (FISA) and the FISA Amendment Act 2008 (FAA)

Within the U.S. statutory framework the Foreign Intelligence Surveillance Act (FISA) provides for the acquisition of foreign intelligence information (50 USC §§ 1801-1885c) by the U.S. authorities.[27] The Patriot Act has amended the statutory powers in various ways. The same is true of the FISA Amendments Act (FAA) of 2008.[28] The FAA is of special importance in the context of this study since 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.[29] These provisions can be found in Section 702 of the FAA and the section thus added to Title 50 USC, Section 1881a (in Title VII – 'Additional procedures regarding certain persons outside the United States') and are explained below. Afterwards certain other powers under the FISA relevant to the subject of this study are considered.

The significance of Title 50 USC, Section 1881a from the Dutch perspective can best be understood by examining 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, as already discussed above. Second, 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, the recent amendments to the FISA (by the FAA) as a reaction to warrantless wiretapping of 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. The FISA can be regarded as a compromise between two conflicting interests: on the one hand, the wish to facilitate the acquisition of foreign intelligence by 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.[30]

The FISA was therefore not intended to protect Europeans or other foreigners from the interception of their communications by U.S. intelligence and national security agencies. Nor was it ever intended that the FISA should regulate the interception of communications of foreigners not located in U.S. territory.[31]

The FAA of 2008 and the provisions of Title 50 USC, Section 1881a are the outcome of a more recent debate in the United States on warrantless wiretapping by the NSA during the Bush administration. The Bush administration had intercepted the communications of Americans without obtaining a judicial

[27] For a concise overview of the provisions of the FISA, see CRS 2007.

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

[29] For an overview (for the European Parliament) of the implications of this provision from a European perspective, see Bowden 2012.

[30] See Banks 2007, pp. 1216-1233.

[31] See Blum 2009, pp. 278-279.

warrant. The New York Times had carried reports on this from late 2005.[32] The debate focused on whether there had been unconstitutional wiretapping of *American* citizens on the pretext of gathering foreign intelligence.

In response to public resistance and the argument of the government entities concerned that the FISA procedures did not provide effective instruments, the U.S. legislator modernized the FISA and regulated these controversial activities by law by introducing the Protect America Act (PAA) in 2007 and the FAA, which replaced the PAA, in 2008. A debate is underway at present in Congress on the extension of the legislation concerned, which would otherwise expire at the end of 2012.[33] The American Civil Liberties Union (ACLU) considers that the FAA is unconstitutional.[34] It should be noted, incidentally, that the FAA is not controversial in the United States insofar as it concerns the collection of foreign intelligence about foreigners located abroad.[35] The debate in the United States focuses instead 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*.

2.2.4 Acquisition of data about non-U.S. persons abroad: Title 50 USC, Section 1881a

Title 50 USC, Section 1881a is the statutory provision under which U.S. intelligence and security agencies gather intelligence information about non-U.S. persons located outside the United States.[36] It provides that a special court known as the Foreign Intelligence Surveillance Court (FISC) should review the acquisition of intelligence information in this way if U.S. government entities require the assistance of electronic communication service providers for this purpose. As is evident from the definitions in Title 50 USC, Section 1881, the relevant powers apply to different kinds of electronic communication service providers, including telecommunications carriers, providers of electronic communication services and providers of remote computing services.[37] Remote computing services entail the provision to the public of computer storage or processing services by means of an electronic communication system.[38] The definition therefore includes cloud computing services. The FAA, unlike the FISA, is technology-neutral.[39] Under the FAA, it therefore 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.

The power to order the acquisition of data under Title 50 USC, Section 1881a rests with the Attorney General and the Director of National Intelligence. On the basis of this provision they may jointly authorize the targeting of persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The authorization may be given for a period of up to one

[32] See Risen & Lichtblau 2005. For an overview see Banks 2010, pp. 1641-1643. See also Blum 2009; Sims 2006.
[33] See, for example, The Washington Post 2012.
[34] See ACLU 2008.
[35] See Blum, pp. 295-296.
[36] For a concise explanation of this provision by the U.S. authorities themselves, see Clapper and Holder 2012.
[37] Title 50 USC, Section 1881 (4).
[38] Title 18 USC, Section 2711 (2).
[39] See also Ohm 2010.

year. However, approval must have been given beforehand by the FISC (50 USC § 1881a(i)(3)), unless there are exigent circumstances (50 USC § 1881a(c)(2)).

Separate judicial approval of the FISC is not required for each individual exercise of the power in Title 50 USC, Section 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 therefore now weaker than before the introduction of the FAA. Before this Act came into force, 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.[40] 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:

> 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 [50 USC § 1881a] has significantly increased the Government's ability to act quickly.[41]

Most safeguards under Title 50 USC, Section 1881a are aimed at ensuring the constitutional protection of U.S. residents and U.S. persons abroad. 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 the U.S. authorities are consistent with the requirements of the Fourth Amendment. It follows that the judicial review by the FISC actually does not provide any legal protection for non-U.S. persons located abroad.

However, there are substantive limitations that can be considered relevant to non-U.S. persons located abroad. The most important for non-U.S. persons located abroad is that the surveillance under Title 50 USC, Section 1881a must be aimed at gathering foreign intelligence information.[42] However, this term is broadly defined in the legislation. It comprises information relating to a foreign power or region in connection with national defense, national security or acts relating to the foreign affairs of the United States.[43]

Acquiring foreign intelligence information need not be the primary purpose of the exercise of the power. It is sufficient if obtaining such information is a significant purpose of the surveillance.[44] This test has become less strict following the enactment of the FAA.[45]

---

[40] Clapper and Holder 2012, p. 4.

[41] Clapper and Holder 2012, p. 4.

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

[43] 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.

[44] Title 50 USC, Section 1804(a)(6)(b). See also Seamon & Gardner 2005, p. 324.

> 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.[46]

As a result of the introduction of the FAA, the requirement that the purpose of the exercise of the power should be to gather information about a foreign power or an agent of a foreign power as defined in Title 50 USC, Section 1801(a), no longer applies. It is now sufficient for the surveillance to be targeted at non-U.S. persons located abroad. Nor does the acquisition of data have to be targeted at specific suspects; it can instead focus on different and more general types of targets such as NGOs, media organizations and geographical regions abroad.[47] Or to put it another way, the purpose could be to collect information about a research group at a given university in the Netherlands.

Owing to the nature of intelligence operations little information is available about how the powers are exercised in practice. The information about the exercise of the power in Title 50 USC, Section 1881a is not in the public domain.[48] Besides review by the FISC there are also the mandatory half-yearly internal reports on the acquisition of data on the basis of Title 50 USC, Section 1881a. However, these reports are secret and are sent only to the special committee for national security in Congress and to the FISC.[49] The public reporting obligation in the FISA does not extend to figures on the use made of Title 50 USC, Section 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.[50] As regards the use of the power in Title 50 USC, Section 1881a it is necessary to rely on the available academic literature. This use has been gauged by the legal scholar Banks in the following terms:

> 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.[51]

In view of the above, the following conclusion can be drawn about the significance of Title 50 USC, Section 1881a for data access requests in the context of cloud computing. It introduces a statutory procedure that allows the broad, programmatic acquisition of data about foreign persons abroad without the need for a suspicion. The acquisition need not be targeted at specific persons or the specific content of their communication, but must contribute to the collection of foreign intelligence

---

[45] For a discussion see Baldwin & Koslosky 2011, pp. 719-720.

[46] Banks 2010, p. 1646.

[47] For a detailed discussion see Banks 2010.

[48] For a Dutch publication discussing the structure of the review of intelligence and security services see the Review Committee on the Intelligence and Security Services 2007.

[49] Heavily censored versions of these reports have been made public as a result of requests under the U.S. Open Government Act and can be found on the Internet. See, for example, Attorney General and Director of National Intelligence 2010.

[50] 205 times in the 2011 calendar year. See Department of Justice 2012. The obligation to publish these data is a consequence of Title 50 USC, Section 1862(c)(1).

[51] Banks 2010.

information.[52] The power can be used in relation to cloud computing services operating in the United States and gives the U.S. government entities concerned the statutory power to gather data on a large scale about non-U.S. citizens located abroad. This is not contrary to the U.S. Constitution.

2.2.5 Other relevant provisions in the FISA

Besides the provisions relevant to the position of non-U.S. persons outside the United States, the FISA includes a long list of specific powers for electronic surveillance (50 USC §§ 1801-1812), physical searches (50 USC §§ 1821-1829) and the production of tangible things and access to certain business records for foreign intelligence purposes (50 USC § 1861). As noted previously, one of the main aims of these provisions is to provide constitutional protection for U.S. persons – protection that is not available for non-U.S. persons located outside the United States.

In its present form, Title 50 USC, Section 1861 is a product of the Patriot Act and enables the FBI to request access to business records for an investigation into espionage and terrorism involving both U.S. and non-U.S. persons. The scope of this provision is therefore more limited than that of Title 50 USC, Section 1881a, which relates to the acquisition of foreign intelligence information in the broader sense. In the case of a U.S. person the investigation may not focus exclusively on activities protected by the First Amendment. However, this may be the case in relation to non-U.S. persons. Examples of these activities would be attending political or religious meetings or writing about certain political or religious subjects. Unlike Title 50 USC, Section 1881a there need not be any involvement of an electronic communication service provider. However, the power could still relate to the provider of a cloud computing service.

The current procedure and possibilities of Title 50 USC, Section 1861 have been modified and some of the safeguards weakened by the Patriot Act.[53] The FBI no longer needs to demonstrate a reasonable suspicion and it is sufficient if there is a terrorism or espionage investigation. The persons targeted by the investigation need not have a link with a foreign power. Title 50 USC, Section 1861(d) also provides for the possibility of imposing gag orders: obligations for businesses not to disclose the exercise of the power by government authorities.

2.2.6 The Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA)

The Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA) which forms part of it (18 USC §§ 2701-2711) regulate government access to electronic communications in the context of criminal investigations and prosecutions by the U.S. judicial authorities, the police and other agencies concerned.[54] To some extent this federal legislation makes up for the absence of constitutional protection due to the third party doctrine already discussed above. It provides procedures for data searches and sets statutory limits for wiretapping and the gathering of data in the electronic communications sector. It also prohibits the voluntary disclosure of these data by the agencies

[52] See Banks 2010. See also Bowden 2012.

[53] See Rubel 2007.

[54] See Kerr 2004.

concerned. As noted previously, the Patriot Act made a number of changes to the ECPA. This concerns legislation that is already some decades' old and is alleged to no longer provide clarity in today's much more complex landscape of electronic communication services.

> It is unlikely that anyone could provide a definitive opinion about the privacy protections available for information in the cloud against a government or other demand for disclosure.[55]

In connection with cloud computing this mainly concerns stored data. The SCA is therefore the most relevant. The provisions on the interception of communications (Title 1 of the ECPA) deal with interception in the transmission phase and will not be considered further here.

The SCA makes it possible for the police and judicial authorities to access stored communications and records of users of electronic communication services and remote computing services.[56] A distinction is made between communication services and remote computing services and also with regard to the length of the data storage. The strongest legal protection is afforded in cases involving a communication service where the communication requested by the police or judicial authorities is less than 180 days' old. In such a case a warrant is necessary in order to access the records and a reasonable suspicion must be demonstrated in the case of each individual search (18 USC § 2703(a)).

Two different procedures apply in the case of remote computing services. There is one procedure for requiring disclosure of contents (18 USC § 2703(b)) and another for requiring disclosure of records pertaining to the user or the use of the service concerned (18 USC § 2703(c)), for example identifying data or the numbers used such as the IP address of an Internet user.[57] It must be shown that there are reasonable grounds to believe that the requested records will be relevant and material to an ongoing criminal investigation.

As noted above, the Stored Communications Act (SCA) limits the possibility for Internet Service Providers (ISPs) to divulge information voluntarily to a government entity (18 USC § 2702). However, an exception is made to this rule for so-called traffic and subscriber data, such as email addresses and IP addresses.[58] In addition, non-public ISPs such as university networks may disclose data voluntarily, whether relating to the contents of communications or otherwise.[59]

In most cases data stored in the cloud will enjoy the protection of the ECPA and the Stored Communications Act, but the precise nature of this protection and whether it is sufficient in terms of the protection of privacy is a matter of debate.[60] To what extent communications and data stored with

[55] Gellman 2009.

[56] A recent legal action in the United States concerns access to the personal records and private communications of a Dutch citizen on Twitter. See U.S. District Court, Eastern District of Virginia, Memorandum Opinion, Case 1:11-dm-00003-TCB-LO, Document 85, Filed 11/10/11,https://www.eff.org/sites/default/files/filenode/MemorandumOpinion1353.

[57] For a more detailed description of the powers in the Stored Communications Act, see Kerr 2004.

[58] 50 U.S.C. sec. 2703(c). Zie Kerr 2004, p. 22-24.

[59] 50 U.S.C. §§ 2702(b) and 2702(c).

[60] See, for example, Dempsey 2006.

electronic communication services enjoy the protection of the Fourth Amendment is a constant source of litigation. In *U.S. v. Warshak* the judges of the Sixth Circuit held on appeal that a person who stores emails on the server of a third party is certainly entitled to a 'reasonable expectation of privacy'.[61] In *Rehberg v. Paulk*, however, the Eleventh Circuit held that stored emails are entitled to the constitutional protection afforded by the Fourth Amendment.[62] The Supreme Court has not yet expressed a view on this matter. Nonetheless, the position remains that if a person whose records have been requested is not a U.S. person and is not located in the United States, he cannot invoke the protection of the Fourth Amendment.

Finally, it should be noted that the statutory framework for the acquisition of data by and the disclosure of data to U.S. authorities is not static and is instead the subject of constant political debate and changes. It follows that the answer to the questions raised in this study can also change in important ways. At the end of 2011, for example, the Cyber Intelligence Sharing and Protection Act (CISPA) was introduced in Congress.[63] The Bill deals with the exchange of information between American companies and the government in the event of cyber attacks. The effect of CISPA would be to compromise the protection afforded by the ECPA against the voluntary disclosure of data by electronic communication services to the government.[64]

2.3 Legislation and constitutional protection in Europe

To put the American statutory and constitutional framework in perspective, this section will briefly consider the comparable legislation and constitutional protection in Europe. The United States is certainly not alone in granting powers to government entities such as the judicial authorities, the police and national security agencies. Nonetheless, there are also various differences that are relevant in terms of legal protection.

Generally speaking, the privacy protection applicable in Europe is laid down in Article 8 of the European Convention on Human Rights (ECHR) of the Council of Europe and Articles 7 and 8 of the more recent Charter of Fundamental Rights of the European Union (Charter). These fundamental rights at European level are the yardstick for assessing the actions of government entities and businesses in relation to any person in the jurisdiction and therefore have a universal character.[65] They protect the right to respect for private life and the right to respect for correspondence (confidentiality of communications), regardless of citizenship, origin or place of residence, which is an important difference from the constitutional protection afforded by the Fourth Amendment in the US.

[61] *Warshak v. United States*, 490 F.3d 455 (6th Circuit 2007).
[62] *Rehberg v. Paulk*, 529 F.3d 892 (11th Circuit 2007).
[63] Cyber Intelligence Sharing and Protection Act (CISPA) H.R. 3523 (19 April 2012).
[64] See Electronic Frontier Foundation 2012.
[65] The Netherlands is a member of both the European Union (for which both the Charter and the ECHR are in force) and the Council of Europe (of which non-EU countries such as Turkey, Russia and Ukraine are also members).

Article 8 ECHR

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The tapping, interception or requesting of stored communications and the related data constitute an infringement of this fundamental right, but may be authorized if they meet the criteria developed by the European Court of Human Rights (ECtHR). An infringement of Article 8 (1) ECHR must serve a 'legitimate interest', be 'in accordance with the law' and 'necessary in a democratic society'. On the basis of Article 8 ECHR the ECtHR has imposed the obligation on European governments to arrange for the powers and safeguards concerning government access to data and the contents of communications to be incorporated in legislation.[66] The arguments generally put forward by the ECtHR are that it should be possible for society to find out about privacy infringements by government entities, that these entities should accurately justify the public interest in requesting disclosure of data and that citizens should be able to defend themselves against the consequences of government access. In view of the above, a second striking difference is that in the European legal order limitations on the right to privacy have to be regulated by law, whereas in the U.S. system privacy protection exists – in the cases in which the Fourth Amendment affords no protection – only where it is regulated by law (e.g. the ECPA).

The European Union has rules governing judicial cooperation, but has for the time being left the adoption of powers in the fields of criminal prosecution and national security to the individual Member States. Before the Treaty of Lisbon, the powers to demand the disclosure of data in a legal sense were exclusively reserved to the Member States, but since the entry into effect of this Treaty the adoption of these powers at European level has become possible.

Hitherto, the European legislator has not introduced rules relating to cloud computing and data access criteria for national government entities. The revision of the Data Protection Directive is of interest in this connection. Whereas strict rules were included in the leaked versions of the new Regulation governing requests for the disclosure of cloud data by foreign government entities,[67] these rules have been watered down in the version of the Regulation finally published.[68] The relevant legislation also contains the provisions introducing conditions for the transfer of personal data to outside the EU, which play an important role in the debate on the legal framework for the entering into cloud computing arrangements in Europe. It is therefore important to monitor these developments in the EU since the European legislator could possibly introduce further rules governing the protection of data of Europeans

[66] See, for example, ECtHR 1 July 2008 (*Liberty v. UK)*, § 62-69.

[67] This concerned Art. 42 (3) of the relevant leaked text. See European Commission 2011.

[68] See European Commission 2012, paragraph 132 of the Preamble.

in the cloud and achieve better coordination between the possibilities for data access requests and the general rules governing the processing of personal data. The Article 29 Working Party, which is the body for consultation between the European privacy supervisory authorities, has noted as follows in this connection:

> Access to personal data for national security and law enforcement purposes: It is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority. [...] The Working Party is concerned by this gap in the Commission proposal as it entails a considerable loss of legal certainty for the data subjects whose personal data are stored in data centres all over the world. For that reason, the Working Party would like to stress the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law.[69]

For the time being, however, the rules governing data access requests to cloud service providers in Europe can be found in the legislation of the various countries. Examination of this legislation shows that there are statutory grounds for data access requests in other European countries which are comparable to the powers of U.S. authorities described above. For example, it has been possible in Sweden since 1 January 2009 to monitor all cross-border telephone and Internet traffic on the basis of the new FRA legislation. The law was passed as part of an antiterrorism package and the Swedish authority which is responsible for this surveillance does not need a warrant for this purpose. In the United Kingdom a bill was recently introduced in Parliament which contains far-reaching new powers for the government to request data on Internet communications (the Communications Data Bill).[70] It should be noted, incidentally, that these statutory rules in Sweden and the UK have not yet been tested by a court for compliance with the ECHR criteria.

2.4 Data access requests in the Netherlands

Just as in the United States, a distinction must be made in the Netherlands between data access for the intelligence agencies (General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD)) on the one hand and access for the police and judicial authorities on the other. The position of the intelligence agencies is laid down in the Intelligence and Security Services Act 2002 (Wiv 2002). This Act regulates the activities of the AIVD and the MIVD. Under Section 64, subsection 2, opening words and (a) of this Act, the Intelligence and Security Services Review Committee (CTIVD) is responsible for supervision of these agencies.

The Intelligence and Security Services Act 2002 gives the AIVD and the MIVD the power to process the personal data of a wide range of persons (Section 13) and contains various provisions regulating the gathering of data. Section 25, subsection 1, authorizes them to carry out, using a technical aid, targeted

[69] Article 29 Working Party 2012, p. 23.

[70] See, for example, Bernal 2012.

tapping, reception, recording and interception of *any form* of conversation, telecommunication or data transfer by means of an automated activity, irrespective of where this takes place. Under Section 27, subsection 1, the AIVD and the MIVD are authorized to receive and record *non-cable* telecommunications on a *non-targeted* basis. In a supervisory report concerning the use of signals intelligence (SIGNIT) by the MIVD, the CTIVD states that in a number of cases consent has been granted for the targeted interception or selection of data of a specific, widely defined category of persons and organizations, and that this procedure is not consistent with the Intelligence and Security Services Act 2002.[71]

The powers of access for the police and judicial authorities are regulated in the Code of Criminal Procedure. The Data Access Requests Powers Act (Wbvg) entered into force on 16 July 2005. This Act confers the power to demand the disclosure of certain data by third parties in the course of a criminal investigation. A demand may relate to identification data, non-identification data, future data or sensitive data. The Act also grants the power to request cooperation in decrypting data. These coercive measures are contained in the Code of Criminal Procedure (Articles 126nc-126nh and 126uc-126uh). The degree of legal protection afforded is on a sliding scale: the more far-reaching the category of data, the stricter are the conditions. For example, the involvement of the public prosecutor is not required in the case of identification data and requests for such data can be made by an ordinary investigating officer.

The powers under the Data Access Requests Powers Act can also be used to gather data about persons other than a suspect if this is necessary in the interests of an investigation. Data may be collected from anyone who can reasonably be required to supply them. In principle, anyone whose data have been stored and processed may be the target of a data access request. The powers under the Data Access Requests Powers Act are therefore wide-ranging. Third parties have a duty, in principle, to supply requested data. Failure to comply with a data access request may constitute the offense of failing to comply with an official order or demand (Article 184 of the Criminal Code). Article 126bb, paragraph 1, of the Code of Criminal Procedure also contains a notification provision. This means that if the situation permits, a suspect or other party involved will be given written notice of the exercise of the powers under the Data Access Requests Powers Act. This duty of notification does not extend to identification data.

In addition, the Dutch government has also made it possible by law, partly through treaties concluded with other States (including the United States), for data about Dutch citizens to be requested by foreign judicial authorities or security agencies for the purposes of investigations. For example, there are the agreements on mutual assistance in criminal matters, on the basis of which the police and judicial authorities can use their powers for the benefit of a foreign government such as the U.S. government. If U.S. government agencies have no jurisdiction over an entity operating in the Netherlands, they may submit a request for mutual assistance under such agreements. From the international law perspective these agreements are the appropriate means by which foreign governments can access data about

[71] See CTIVD 2011, sections 7.2.2. and 8.3.3.

Dutch nationals.[72] However, in the case of a cloud provider (or associated company) whose activities in the United States are of a continuous and systematic nature, there is no clear obligation under U.S. law for the U.S. government to rely on such agreements when seeking access to data on non-U.S. persons in the Netherlands. In principle, the U.S. government itself simply claims jurisdiction in cases of this kind, as discussed in section 2.1 above. Naturally, this does not exclude the possibility of achieving a more balanced arrangement through international conventions.

Under Section 59 of the Intelligence and Security Services Act 2002 it is also possible for Dutch intelligence and security agencies to supply data voluntarily to their foreign counterparts and, at the request of intelligence and security agencies of friendly nations (such as the United States), to provide assistance. Such assistance may involve the exercise of special powers such as wiretapping and data access requests to Dutch organizations or businesses. The CTIVD noted recently that in such circumstances the Dutch agency concerned should independently assess whether the exercise of the powers is consistent with the Dutch conditions. But it is apparent from the same report of the CTIVD that in practice such assessments are not always made properly and that, in the field of signals intelligence, assistance is generally provided on the basis of 'Memoranda of Understanding'.[73]

[72] For a discussion and recommendations on this point see Brown & Korff 2012. See also Westmoreland 2012.

[73] CTIVD 2011, pp. 59-60.

3. Implications of U.S. statutory data access framework when using cloud services

To ensure that the legal analysis is clear in practice, the main conclusions are listed below. In addition, three scenarios for accessing data stored in the cloud are provided. Section 4 then considers how these legal conclusions relate to the legal framework in the United States and assesses the risks of data access requests in the context of other legal and information security considerations that play a role when deciding whether to migrate IT functions and data to cloud-based computing services.

The above overview of the statutory framework and the constitutional protection in the United States shows that it is possible for the U.S. authorities to gain access to cloud data of foreign higher education and research institutions in the context of criminal investigations and that there are few substantive barriers for U.S. intelligence agencies in this regard. Title 50 USC, Section 1881a is the most striking provision in this respect owing to the procedures it regulates and the underlying lack of legal protection for non-U.S. persons located outside U.S. territory. In principle, this provision makes it possible to acquire data and communication records of large groups of Dutch citizens using cloud-based computing services from any given provider that conducts activities in the U.S., without information about such practices becoming available for the users of the service or the individuals concerned. Such data acquisition does not have to be targeted at foreign intelligence information exclusively. It is merely necessary that the acquisition of foreign intelligence information was the main purpose of such data access requests.[74]

Scenario 1: Student data

As part of a course of an interdisciplinary master's degree program in Digital Media at a Dutch university, teams of students are required to write papers on the possibility of guaranteeing the confidentiality of whistleblowers at websites such as Wikileaks. The lecturer is a recognized international expert on the use of cryptographic techniques by journalists and activists. Developers of a new Wikileaks site who are interested in the ideas developed by the students attend an evening seminar held during the course. The university concerned uses the cloud computing services of a large U.S. service provider for the great majority of the available ICT functions for students, such as document storage, email and the e-learning environment.

The physical location of the servers on which the U.S. service providers store their data is not relevant to the question of whether U.S. legislation allows access to the student data. Under Title 50 USC, Section 1881a the competent U.S. authorities, such as the National Security Agency (NSA), can, in principle, gain access to the data of the entire student population of the university concerned held by the provider, for example for the purpose of acquiring foreign intelligence information about threats to the security of the United States.

There are no constitutional safeguards in the United States for Dutch users of cloud computing services who are subject to U.S. jurisdiction, since the Fourth Amendment is not applicable. First of all, as cloud providers can be designated as third parties the users of their services typically do not have any

[74] For a recent discussion of the national security problem by the Director of National Intelligence, see Clapper 2012.

'reasonable expectations of privacy' under the Third Party doctrine. Moreover, U.S. constitutional safeguards do not extend to foreigners who are not located in the United States. From the U.S. legal perspective, Dutch users of cloud-based computing services therefore enjoy the same degree of constitutional protection as North Koreans.

Furthermore, the physical location of the servers is, in principle, irrelevant to the powers of the U.S. authorities as jurisdiction exists in relation to a business if its activities in the United States are of a continuous and systematic nature, such as a subsidiary or branch. As noted before, the existence of a direct link between jurisdiction and the location of the storage is an incorrect but widely held assumption in the debate. Indeed, it is an assumption that crops up in various research reports, for example the study on cloud computing of the authoritative European Network and Information Security Agency (ENISA).[75]

Scenario 2: Management information in emails

The board of a large Dutch university of applied sciences is engaged in talks about cooperation and student exchanges with a number of technical universities in the Gulf region. An American consultant is called in to assist with shaping the joint venture. The management emails with the foreign partners of the Dutch university are stored in the UCloud, a cloud computing service provided by UniSer. Data in the UCloud are only stored on servers in the Netherlands. UniSer, which is based in the Netherlands, also provides a cloud computing service known as UCalCloud in the United States and has a branch and data centers in Utah.

Although in this scenario the emails are stored on servers in the Netherlands, this is irrelevant to the scope of the U.S. legislation regulating the acquisition of such data. What is relevant is that UniSer also provides services in the United States. Had it not, U.S. authorities would not, in principle, have direct access to the data when conducting foreign intelligence operations. In such cases, the assistance of the Dutch intelligence agency can be requested. If the American consultant were the subject of a criminal investigation, the management emails could be requested by U.S. authorities in three ways: (1) through voluntary disclosure by UCalCloud; non-public ISPs (e.g. university networks) may supply either content or communications data voluntarily to judicial authorities, but voluntary disclosure may be subject to contractual limitations; (2) through a request under Title 18 USC, Section 2703; in the case of a non-public ISP the Stored Communications Act is not applicable (50 USC § 2711 in conjunction with 50 USC § 2703), so the data can be obtained with an ordinary subpoena; (3) through a request for mutual assistance, in which the U.S. authorities ask their Dutch counterparts to obtain data from UCloud, or from the university itself.

The relevant provision of the FISA (50 USC § 1881a) contains few if any conditions and limitations that constitute a meaningful barrier to access to cloud data of foreign users. This condition is amplified by an increasingly blurred legal distinction between law enforcement agencies and intelligence agencies in the United States and the fact that the acquisition of intelligence information need no longer be the primary purpose of the exercise of government power, merely a significant purpose. It follows that data

[75] The ENISA study is based on the assumption that the storage location determines whether or not there is jurisdiction. See ENISA 2009, p. 84.

requested and acquired for intelligence purposes may, in principle, end up in the possession of law enforcement agencies. In other words, these agencies may obtain information not only about a student who could pose a threat to U.S. national security but also about a student who makes an appointment in good faith through email with a person suspected by U.S. authorities of drug trafficking.

> Scenario 3: Research group and nuclear research data
>
> A research group at a Dutch university of technology is conducting research into new developments in the field of nuclear technology. The group's research data have recently been put on the EUcloud, an EU-wide cloud service operated by and for universities. The EUcloud servers are located in Germany. EUcloud has been established as a private organization. However, EUcloud gets into financial difficulties and puts itself up for sale. It is ultimately acquired by a larger player in the cloud computing market with subsidiaries in the United States. Another candidate was a cloud provider that has its head office in China.
>
> If there is no link between EUcloud, the university and the United States, U.S. authorities do not have direct access to these research data. However, it is conceivable that, in the course of international contacts about nuclear proliferation, U.S. intelligence agencies may obtain data indirectly from friendly European services, including the Dutch intelligence agency AIVD. The ECHR and the EU Charter of Fundamental Rights provide constitutional legal protection for persons who are screened by these agencies or whose personal data are gathered by them in the course of operations. After the takeover of EUcloud, however, the United States obtains jurisdiction. Access to data for judicial authorities or intelligence and security services cannot be excluded contractually. However, this is possible with respect to a client's legal position in the event of takeovers for example if such a takeover would open up access to data from other jurisdictions.

For the time being, the EU has left the statutory regulation of data access powers to the Member States. National security and law enforcement are recognized grounds for exceptions to privacy and data protection rights in the Netherlands and other EU Member States, which can in principle legitimate wide-ranging data access powers. A major difference with the current situation in the United States is that in EU Member States data access powers are circumscribed by broadly defined fundamental rights. The ECHR and the EU Charter of Fundamental Rights, which recently entered into force, require protection of individual legal rights (such as the right to a fair trial) and a certain degree of transparency and accountability in relation to wiretapping and data access more generally. An additional difference between the constitutional frameworks in the EU and the US is that European fundamental rights are of a more universal nature (applicable to everyone, irrespective of nationality or place of residence), whereas non-U.S. nationals outside U.S. territory receive little if any protection under the statutory framework in the United States. Third, as already noted, privacy limitations in Europe must be provided for by legislation, whereas privacy protection in the United States is not a given. In view of the limited applicability of the Fourth Amendment, the situation in the U.S. is often the reverse. There, privacy protection is regulated by law in specific contexts, for example in the Electronic Communications Privacy Act (ECPA).

When considering these similarities and differences between the U.S. and European jurisdictions with regard to cloud computing and data access, it must first of all be noted that there are no legal guarantees for the confidentiality of information in the cloud. If law enforcement or intelligence agencies in the Netherlands or a friendly nation have reason to seek access to data, they are generally able to obtain this in one way or another. If data are stored with cloud providers that conduct activities in the United States, it can be argued that the current legal framework the makes it possible for the authorities to obtain the data directly from the provider in almost all conceivable situations.

Whereas data access possibilities exist in both jurisdictions, data stored in cloud environments that are entirely separate from 'activities conducted in the United States' receive additional legal protection on the basis of the ECHR and the EU Charter of Fundamental Rights. In practice, however, it will not always be easy to discover whether a cloud computing service or any of its partners in its value chain have activities of a continuous and systematic nature in the United States, such as a subsidiary or branch. Clearly, this will be the case for many cloud computing service providers that operate internationally and, even where these activities do not exist, the situation could change at any time as the result of mergers and acquisitions. From the European and Dutch perspective, the additional legal protection for services that do not fall under U.S. jurisdiction deters the enactment of unduly far-reaching data access powers and the further use of these data for various security objectives.

4. Risks

4.1 Data retrieval from the cloud: theory and practice

The previous section noted that there are no legal safeguards to guarantee the confidentiality of cloud data requested by the U.S. government if the cloud provider in question 'conducts business in the United States'. In the case of data of non-U.S. persons, there is, moreover, a lack of transparency as to how often, by which authority and for which reasons access to cloud data is requested by U.S. government authorities. Access is typically requested for the acquisition of intelligence information and for the purpose of criminal investigations. It is to be expected, however, that initiatives in the area of cyber security, such as CISPA – with its broader definitions and scope – will extend the powers of access to and frequency of requests for access to cloud data.

In its extensive report about the advantages and risks of cloud computing, ENISA stated as early as in 2009 that the risks relating to data access requests from other jurisdictions are high.[76] Note in this respect that in 2009, ENISA still assumed a link between jurisdiction and the location of the storage and that the physical location of information is therefore relevant to the scope for data access by government entities. However, based on the rules governing jurisdiction described in section 2, the physical location is mostly irrelevant in the American context. This has made the mitigation of this risk all the more complex.

The practical question that follows from the high risk and more complex mitigation, is of course how often access to information is actually requested. The fact that it is possible to request access to data from a cloud provider does not mean that such requests will actually be made. Reliable estimates of actual requests cannot be given, as there is no obligation in the United States to report about data requests regarding foreigners. It is therefore not possible to provide quantitative information about actual data requests nor to describe trends in the acquisition of data from cloud providers with international operations. Note that an advantage of strict in-house data management is that the institution concerned will in principle have insight into the number of data requests, as such requests are made to the institution itself. In other cases, a general idea of actual data requests now and in the future can be obtained through conceptual observations.

Lawful access to data stored in the cloud is already gaining ground in the context of intelligence information acquisition and criminal investigations, and the relevance of access to cloud data for national security purposes is expected to grow in the future. Without aiming to be exhaustive, several trends can be discussed. First, the adoption of cloud services is growing spectacularly. As a result, more relevant information can solely be retrieved from the cloud. Furthermore, methods of analysis are becoming more sophisticated, so it pays for authorities to mine large amounts of data for patterns, for example of suspicious behavior.

[76] ENISA 2009, p. 45-46.

Secondly, in addition to the endogenous developments that are inherent to cloud computing, several exogenous factors are contributing to the growing importance of cloud data for intelligence and law enforcement purposes. The effectiveness of established means of data access is being eroded. A case in point is wiretapping of electronic communications. As early as in 2005, an evaluation report of the Dutch Telecommunications Act underlined that due to "several technological and market developments, the effectiveness and efficiency of legislation governing wiretapping is declining".[77] Whereas the market trends concerned include decentralization and an explosive growth of electronic communications providers, the technological trends relate to packet-switched information transmission (rather than circuit-switched), where wiretapping is possible only at the end points of the network – close to end users. This wiretapping method is costly, as communications need to be tapped at a multitude of points, as opposed to a central switch in the network. This applies similarly to law enforcement access to data.

Another important trend is the wide availability and standard use of encryption in real-time communications, such as the use of encryption for web browsing and email traffic. Whereas conventional telecommunications providers are required by law to set up their networks to facilitate lawful access to data and wiretapping, end-to-end encryption makes that such communication is not, or only barely noticeable for telecommunications and internet service providers. For web mail providers, HTTPS communication is currently the standard, so communication cannot be effectively intercepted in transit except at the webmail provider itself.[78] The American privacy expert Swire has described this development and states that the attention of intelligence and law enforcement agencies will shift to cloud providers. 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. This applies to all types of cloud computing for the general public, including VoIP, webmail, e-commerce, banking and a whole host of other applications.[79] A possible consequence of this development is that information will increasingly be encrypted on servers as well.

Regarding the number of requests, the American legal scholar Banks makes a distinction between the various stages of the communication process. He reckons that the U.S. government uses a broad 'vacuum-cleaner approach' for the acquisition of stored data and that the National Security Service (NSA) subsequently analyzes the data collected.[80] In this context, U.S. legal scholar Swire refers to recent reports about a new NSA analysis center that can potentially collect all information relevant to the United States, filter the data to identify patterns and further analyze it.[81] As no official information is available on the developments described by these experts, these cannot be confirmed nor denied. But based on these developments, one may expect that access to cloud data by U.S. authorities will continue to increase.

[77] TILT & Dialogic 2005, p. 67-69.
[78] See Swire 2012 p. 7-10.
[79] See Swire 2012, p. 10
[80] *Supra*, note 46.
[81] See Swire 2012, p. 8. See also Bradford 2012.

4.2 Significant risks put in perspective

In general, this report brings to light that there are limits for institutions of higher education and research to legally safeguard the confidentiality and security of data once they engage cloud computing services from providers who 'conduct business in the United States'. Neither contractual agreements nor general legal provisions in the Netherlands can change this undesirable situation for these institutions. In this specific sense the use of cloud computing services curtails the autonomy, control and the information position of the institutions, which may jeopardize the intellectual freedom of staff and students in higher education in the Netherlands. The fact that the confidentiality of information cannot be guaranteed may damage the reputation of these institutions. Additionally, the transition to cloud computing could create new opportunities for the U.S. government to access information in the future (*function creep*). The threat of actual access to data is permanent and may negatively affect the extent to which scholars are willing and able to communicate (*chilling effect*).

The above observation has concrete implications. Higher education and research institutions will not be able to inform their staff or students of actual data requests, let alone be able to protect their staff from national security or criminal investigations by U.S. authorities once information is requested. If data is processed in-house, institutions will at the very least know of such investigations at an early stage. Excesses with regard to individual surveillance or possible surveillance of a research group, as described in the scenarios in Section 3, would embarrass educational institutions and might damage their reputation. In such circumstances, cloud computing challenges the societal responsibility of institutions.

Institutions of higher education and research should realize that they cannot build a relationship based on trust with the cloud provider when it comes to data requests by foreign governments. They can never be sure exactly how cloud providers process their data when faced with data requests, and cannot inform themselves whether or not cloud providers cooperate closely with government entities in this respect.[82] This asymmetry in the information position is a risk and stands in the way of careful decision-making about the use of cloud services. It remains to be seen, for example, whether higher education and research institutions will ever have complete insight into the 'activities of a cloud provider in the United States', 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 a desired termination of agreement. It is neither in the interest of cloud providers nor their duty to remove this asymmetry. Moreover, cloud providers may not be in a position to provide an answer in good faith on these complex

[82] A recent example is the ruling of the District Court Virginia in EPIC vs NSA concerning the cooperation between Google and the NSA. The court ruled that neither Google nor the NSA need to confirm or deny whether they cooperate. See *EPIC v. NSA*, 11-5233 (6th Circuit 2012), http://www.wired.com/images_blogs/threatlevel/2012/05/EPIC-v.-NSA-DC-Cir.-2012.pdf. See also Kravets 2012.

issues, let alone any guarantees. 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.[83]

The risks of law enforcement access to data that arise from migration to the cloud by SURF and other higher education and research institutions in the Netherlands are significant. Yet these risks need to be seen in perspective. Without attempting to be exhaustive, we will reflect on the risks discussed above from the perspective of information security policies in general and data access requests in particular.

Institutions of higher education and research may be of the opinion that data access requests by government agencies pose hardly any problems with regard to certain categories of data. To what extent do requests for public information and non-sensitive information constitute a risk for higher education and research institutions or for end users? This question raises an important consideration that needs to be addressed when deciding whether or not to move into the cloud, namely which categories of data are deemed to be sensitive by educational institutions and end users. In other words, which factors cause that invisible and possibly even uncontrolled government access constitutes a risk for higher education and research institutions? This question is not related to the desirability of such access, but it is all the more pressing given the legal state of play and the perceived benefits of cloud computing for higher education and research institutions.

A second perspective on the protection against risks arising from cloud use relates to end users. Educational institutions are free to decide for themselves not to use cloud services. Having said that, if an end user communicates with a third party that makes use of cloud computing services, the protection offered by in-house data processing can no longer be guaranteed. End users seldom know in what ways their data are processed by third parties – for example, whether an American cloud provider is involved. A host of universities across the globe have opted for the processing and storage of data in the cloud, using services often offered by American cloud providers. And if data processing practices are more widely known, such as is the case with the University of Cambridge, which has been using Google's cloud services for some time now,[84] it is still open to question whether this knowledge will deter scholars from communicating or even collaborating with scholars who work at those institutions. Data that have been consciously protected by an educational institution may still become available to government authorities via this route. These practical circumstances truly limit the possibility to protect data against data access requests in the cloud.

Given the analysis presented in this study, higher education and research institutions should consider data access requests in any risk assessment of using cloud services. In practice, however, it is difficult to determine the weight of data requests in the long list of risks related to information security. Data leaks, the actual removal of data after deletion by end users and the interoperability of encryption standards are not only relevant security risks in the context of lawful or unlawful government access, but could in themselves constitute an even greater risk for higher education and research institutions, as well as for

[83] So-called SaaS providers (Software as a Service), as opposed to IaaS (Infrastructure as a Service). See for further details SURFNET 2010, p. 3-4.

[84] See University of Cambridge 2012.

the privacy and information security of end users. And whereas the ENISA study referred to above puts government access in the highest risk category, it is beyond the scope of this study to look into the broader information security perspective in more detail. Nonetheless, institutions of higher education and research should seriously consider the risks related to requests for access to data stored in the cloud.

5. Conclusion and recommendations

5.1 Conclusion

What are the implications of the Patriot Act for the possibility that access to information from Dutch higher education and research institutions stored in the cloud is requested by U.S. authorities? This is the key research question addressed in this report.

Prior to addressing this question, one has to note that the Patriot Act has come to play a symbolic role in the debate about whether the confidentiality and security of information stored in the cloud can be sufficiently guaranteed. The Patriot Act, enacted in 2001, has strengthened the powers to acquire data by American intelligence agencies and law enforcement authorities. In practice, however, the Patriot Act is merely a complex part of an even more complex and dynamic system of data access powers granted under the American legal system. Any sensible discussion about the meaning and relevance for higher education and research institutions in the Netherlands of the possibility of the United States acquiring data should be based on an analysis of this broader framework.

Looking at the legal framework in the United States from the perspective of Dutch users of cloud services, the following conclusions can be drawn. First, the United States does not provide constitutional protection where it concerns the acquisition of data of non-U.S. persons located abroad. As a result, any legal protection needs to be regulated by statute. The existing statutory protection relating to the various powers to request the disclosure of data mainly concerns the rights of U.S. persons.

The U.S. government has ample possibilities to request data from foreign (in this case Dutch) users of the cloud. The most striking example in this regard is the specific provision (50 USC § 1881a) introduced in 2008 for the acquisition of data of non-U.S. persons outside the United States, given the far-reaching powers it grants to retrieve information on a large scale, including access to complete data sets. U.S. authorities also have powers to request information from cloud providers in the context of criminal investigations. Jurisdiction under U.S. law is a necessary precondition, which is effectuated when cloud providers are based in the United States or if they conduct continuous and systematic business in the United States. It is a misconception that U.S. jurisdiction applies only if the data are physically located on U.S. territory.

European and Dutch privacy laws (such as the Dutch Data Protection Act, Wbp) offer no safeguards against the exercise of these powers by the U.S. government. Nor can this risk be eliminated by contractual agreements. Whereas contracts would otherwise offer a solution in terms of providing a legal framework for risks, it is not possible from a legal point of view to use them to restrict the powers of law enforcement or intelligence agencies. From an international legal perspective and given the importance of the confidentiality of information for higher education and research institutions, these conclusions give cause for concern. At the end of the day, however, a real solution can only be found at an international level.

In practice, little can be said about the question as to how often the U.S. government will actually exercise the powers described. There is little or no transparency about the exercise of these powers and the cloud service providers in question typically face legal obligations of secrecy, also with respect to those immediately concerned. This makes it difficult to assess the risk that data will actually be requested. At the same time, one may expect that requests for information from cloud providers will become an increasingly important weapon in the arsenal available to intelligence and security agencies. In view of the lack of transparency about data access requests, the transition to cloud computing could lead to a lower degree of autonomy for higher education and research institutions. Conversely, educational and research institutions that manage their data in-house will have an idea of the actual number of requests and may have legal remedies to oppose a data access request.

The fact that the U.S. government has the powers described above to request access to data from cloud providers who conduct business in the United States is not unique in itself. In The Netherlands and in other European countries, too, similar powers are in place. These powers are also exercised on behalf of other countries, such as the United States, in cases where these countries have no jurisdiction over the data sought. Official reports by the Dutch Intelligence and Security Services Review Committee (CTIVD) suggest that in some cases these powers are too easily exercised. An important difference is that Europe offers additional constitutional protection, provided for in the ECHR, and that powers and the exercise of these powers should respect the principle of proportionality guaranteed in the human rights treaty. It is also to be expected that the constitutional interests of Dutch residents will play a more prominent role in the accountability measures taken by Dutch government authorities, such as the accountability of intelligence agencies towards the Dutch parliament and the CTIVD.

5.2 Recommendations

The legal framework discussed, the available risk analyses such as the one conducted by ENISA, and the policy trends outlined in this study provide sufficient reason to take the possibility of data access being requested by U.S. authorities seriously. It is clear that the risk of data access requests by government entities in general should be placed firmly on the agenda. To start with, well-informed decision-making is essential. All cloud providers operating in the Netherlands face the possibility that the U.S. government, another foreign government or the Dutch government request data from the Netherlands. As this is a real possibility, it should be carefully considered and discussed with the providers. Issues that need to be addressed in relation to the United States are, among other things, whether the provider is subject to U.S. jurisdiction, whether some of the services are outsourced to third parties (for example for the purpose of making backups), how the actual removal of data stored in the cloud is organized and what happens with information processed in the cloud in the event of bankruptcy or takeover of the cloud service provider or termination of agreement. If institutions of higher education and research choose to purchase the services of a particular cloud provider precisely because it is not subject to U.S. jurisdiction or to that of another foreign country, the inclusion of a restrictive clause in the contract is recommended, specifying the provisions that apply in the event of a takeover, as such specific preconditions might change.

In addition, it is recommended that higher education and research institutions conduct a thorough risk analysis based on a classification of the various types of data that may be subject to requests. Such internal analyses could then be used by the institution to explain the choices it makes and, if need be, to discuss them with the parties concerned. It would be advisable for the sector to develop alternatives for information and data that might pose too great a risk if they were to come into the possession of an American intelligence or law enforcement agency in a non-transparent manner. A legally sound national cloud for the education and research sector could offer better guarantees against the risk that foreign governments gain excessive access to data.

Most higher education and research institutions already have more or less formalized protocols in place describing how to deal with data access requests by the Dutch law enforcement or intelligence agencies. These protocols and the underlying considerations can play an important role when formulating policies for the transition to cloud services and the related risks of the availability of information to foreign governments. Uniformity in the development and application of protocols is of paramount importance, also where solutions are sought at a national level. Voluntary disclosure of information – which leads to arbitrariness and the undermining of trust – should not take place. Strengthening current regulation in this area could be an appropriate means to achieve this.

Where watertight legal guarantees against undesired data access requests by foreign governments are lacking, technical protective measures can, to an extent, offer meaningful protection. Well-designed decentralized and distributed storage can, for example, prevent all too easy instant access to an entire dataset of one organization. Indeed, the possibility of using encryption should be considered. A caveat in this context is that encryption techniques could lead to overly complex processes for many users. When dealing with highly sensitive information, users need to be provided with clear instructions – this applies equally to data stored in the cloud and to information stored in a more traditional ICT environment within the institution. In order to guarantee proportionality and effectiveness, it is advisable to differentiate data based on their nature and the way in which data flows are processed.

In sum, given the key role of higher education and research institutions in today's society, their transition to cloud computing should be part of a broad cost-benefit analysis that addresses all social and economic interests that are at stake. In doing so, aspects that are not ICT-related and connected to the security and confidentiality of information should be given due attention (academic freedom, reputation, chilling effect).

The various possibilities of the U.S. authorities to request access to data from cloud providers are not a static given, but the topic of constant debate and subject to change. This also holds true when the issues discussed are considered in a broader perspective than merely in relation to the United States. The autonomy of higher education and research institutions in terms of their information management needs to be guaranteed and lock-in should be avoided. Continuously rethinking and coming up with alternatives for the existing situation is imperative. New insights should inform the renegotiation of existing agreements. Guaranteeing a realistic exit strategy is just as relevant in this respect as ensuring the creation of data backups and guarantees that data will actually be removed from cloud servers.

As the regulatory decision-making process discussed in this study is shaped outside the scope of the higher education and research sector, the sector should seek to develop a clear position in the political arena. The protection of privacy and data confidentiality in the context of cloud computing is currently on the EU's political agenda. Part of the debate is about the implementation of better safeguards in relation to requests for access by non-European governments to data stored in the cloud. Incidentally, the powers to acquire data from non-U.S. persons located outside the United States are now also the subject of debate in the United States. The data confidentiality concerns of non-U.S. persons have so far not been addressed in these discussions.

Like any other new technology, cloud computing has its opportunities and threats. Whereas the opportunities are evident, the threats and information about these threats may be obscured in the debate on the subject. To date, the public debate about the USA Patriot Act and its implications for the transition to cloud computing would appear to be an example of the latter. Institutions of higher education and research are ideally positioned to take responsibility in this matter.

References

ACLU, 'Why the FISA Amendments Act is Unconstitutional', 5 February 2008, http://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf.

Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, 10 February 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Article 29 Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196, 1 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

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: June 1, 2009 -November 30, 2009,

May 2010, http://www.fas.org/irp/agency/doj/fisa/sar-may10.pdf.

Jennifer Baker, Europe cloud vendors cleaning up with data protection fears, Techworld, 5 December 2011, http://news.techworld.com/security/3322757/europe-cloud-vendors-cleaning-up-with-data-protection-fears/

Fletcher N. Baldwin & Daniel R. Koslosky, 'Mission Creep in National Security Law', 114 West Virginia Law Review 2011.

James Bamford, Big Brother is Listening, Atlantic Magazine, April 2006, http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/4711/?single_page=true

William Banks, 'The Death of FISA', 91 Minnesota Law Review 1209, 2007.

William Banks, 'Programmatic Surveillance and FISA: Of Needles in Haystacks' Vol. 88 (2010) Texas Law Review 7, 1633-1667.

Paul Bernal, 'The Draft Communications Bill and the ECHR', UK Constitutional Law Group, 11 July 2012, http://ukconstitutionallaw.org/2012/07/11/paul-bernal-the-draft-communications-bill-and-the-echr/.

Rutger Betlem, 'Hoe veilig zijn min data eigenlijk in de cloud?', Expertpanel, Het Financieele Dagblad, 25 juni 2012.

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.

C. Bowden, 'Data Protection for the Digital Age', Greens/EFA Hearing, European Parliament, Brussels, 28 June 2012, http://www.greens-efa.eu/fileadmin/dam/Documents/Events/2012-06-28_Data_protection_for_the_digital_age/Caspar%20Bowden.pdf.

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.

Ian Brown and Douwe Korff, 'Digital Freedoms in International Law', Global Network Initiative, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2085342.

Ronald Bruins, 'Wet- en regelgeving kan cloudaanbieders helpen', Cloudworks, Mei 2011, www.cloudworks.nu/uploads/CW4-los-low.pdf.

James R. Clapper, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, 31 January 2012, http://intelligence.senate.gov/120131/clapper.pdf.

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.

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.

CTIVD, Toezichtsrapportage inzake de inzet van SIGINT door de MIVD, CTIVD nr. 28, 23 August 2011.

James X. Dempsey, 'The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age', Statement before the Senate Committee on the Judiciary, 22 September 2010, https://www.cdt.org/files/pdfs/20100922_jxd_testimony_ecpa.pdf.

Department of Justice, 'USA PATRIOT Act: Sunsets Report', April 2005, http://www.justice.gov/olp/pdf/sunsets_report_final.pdf.

Deptartment of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations (2009), p. 115-116, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

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.

Electronic Frontier Foundation, 'Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It', 15 April 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it.

European Commission, 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), Version 56, 29 November 2011 (Leaked Draft), http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

European Commission, 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), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD).

European Network and Information Security Agency, 'Cloud Computing Risk Assessment' (Rapport 2009) http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

European Network and Information Security Agency, 'Security and Resilience in Governmental Clouds - Making an Informed Decision' (Rapport 2011) http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/

Anna Fielder et al. , Cloud Computing, Study, Directorate General for Internal Policies, IP/A/IMCO/ST/2011, 18 May 2012.

Robert Gellmann, 'Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing', World privacy Forum, 23 February 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

William E. Kennard, United States Ambassador to the European Union, Remarks at the 2012 European Cloud Computing Conference, 12 March 2012, http://useu.usmission.gov/kennard_032112.html.

Orin S. Kerr, 'Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't' 97 Northwestern University Law Review 2003.

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.

David Kravets, Court Upholds Google-NSA Relationship Secrecy, Wired.com, 11 May 2012, http://www.wired.com/threatlevel/2012/05/google-nsa-secrecy-upheld/.

Hogan Lovells, A Global Reality: Governmental Access to Data in the Cloud, A Hogan Lovells White Paper, Washington, DC, 23 May 2012, http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20%281%29.pdf.

NIST, Mell, P. & Grance, T., The NIST Definition of Cloud Computing, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws', 88 Texas Law Review 1685, 2010.

David Saleh Rauf, PATRIOT Act clouds picture for tech, Politico, 29 November 2011, http://www.politico.com/news/stories/1111/69366.html.

Review Committee on the Intelligence and Security Services, *Accountability of intelligence and security agencies and human rights*, The Hague, 2007.

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.

A. Rubel, 'Privacy and the USA Patriot Act: rights, the value of rights, and autonomy', 26 Law and Philosophy 119, 2007.

Paul Schwartz, Reviving Telecommunications Surveillance Law, 75 University of Chicago Law Review, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116783.

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 2005.

John Cary Sims, What NSA is Doing… and Why It's Illegal, 33 Hastings Constitutional Law Quarterly 101, 2006.

Daniel J. Solove, The Digital Person, New York: NYU Press, 2004.

SURFNET, Cloud Security, Checklist en de te stellen vragen, December 2010, http://www.surfnet.nl/Documents/rapport_201012_Cloud_Security_checlist_v1.0.pdf.

Peter R. Swire, 'From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud', 12 April 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871.

David Teneyuca, 'Internet Cloud Security: The Illusion of Inclusion', Information Security Technical Report (2011).

The Washington Post, Top Secret America, 2011, http://projects.washingtonpost.com/top-secret-america/.

The Washington Post, 'Oregon senator blocks five-year extension of surveillance law', 11 June 2012.

TILT & Dialogic, Aftapbaarheid van telecommunicatie, Een evaluatie van hoofdstuk 13 Telecommunicatiewet, Tilburg, november 2005, http://www.dialogic.nl/documents/2004.59-0535.pdf.

TILT, 'De wolk in het onderwijs, Privacy aspecten bij cloud computing services', Surfnet, Kennisnet, 2011, http://www.surf-academy.nl/media/Seminar%20Privacy/De_wolk_in_het_onderwijs_feb2011[1].pdf

Andreas Udo de Haes, 'Amerika graait in Europese clouddata', Webwereld, 1 July 2011, http://webwereld.nl/nieuws/107156/amerika-graait-in-europese-clouddata.html.

University of Cambridge, University Computing Service, Introduction to Google Apps @ Cambridge, 2012, http://www.ucs.cam.ac.uk/googleapps.

U.S. District Court, Eastern District of Virginia, Memorandum Opinion, Case 1:11-dm-00003-TCB-LO, Document 85, Filed 11/10/11,https://www.eff.org/sites/default/files/filenode/MemorandumOpinion1353.pdf.

Van Doorne, Rand Europe & Verdonck Kloosters & Associates, Cloud Computing, Fundament op Orde, Eindrapportage, 2012.

Kate Westmoreland, Sharing Evidence across Borders: the Human Rights Challenge, 2012 (forthcoming).

Zack Whittaker, Microsoft admits Patriot Act can access EU-based cloud data, ZDNet, 28 June 2011,

http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.