EUROPEAN PROTECTIONISM IN CLOUD COMPUTING: ADDRESSING CONCERNS OVER THE PATRIOT ACT

By John T. Billings[‡]

I. INTRODUCTION

In recent years, both individuals and companies have embraced cloud computing as the future of information technology ("IT") architecture.[1] An estimated seventy-six percent of Americans use cloud computing services today,[2] and its use by businesses is estimated to more than double in the next three years.[3] Many companies around the world now outsource data storage and processing to "the cloud,"[4] seeking to save money on IT infrastructure costs, while benefiting from greater access and flexibility offered by the cloud.[5]

[‡] J.D. and Institute for Communications Law Studies Certificate Candidate, May 2013, Catholic University of America, Columbus School of Law. The author would like to thank his family for their continuous support, as well as the *CommLaw Conspectus* staff for their hard work throughout the writing process.

[1] Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust With United States Companies*, 16 J. TECH. L. & POL'Y 229, 230 (2011).

[2] Andrew R. Hickey, *Cloud Computing Befuddles Consumers, Despite Use: Study*, CRN (Aug. 9, 2011, 1:45 PM), http://commcns.org/13JsYWF (citing results of a recent study on "consumer familiarity" with cloud computing).

[3] Maggie Holland, *IBM Pulse 2012: Cloud Computing Use To Double By 2015*, ITPRO (Mar. 7, 2012, 9:26 PM), http://commcns.org/Xfo24V.

[4] The term "the Cloud" stems from computer network diagrams that depict the Internet as a vast cloud at the top of a network chain. *Cloud Computing*, ELEC. PRIVACY INFO. CTR., http://commcns.org/SSl37q (last visited Nov. 10, 2012). For present purposes, "the Cloud" refers to remote servers owned and operated by providers and made accessible to users by the Internet. Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing 4 (Feb. 23, 2009), *available at* http://commcns.org/WLrmoy.

[5] Mladen A. Vouk, *Cloud Computing—Issues, Research and Implementations*, 16 J. COMPUTING & INFO. TECH. 235, 235 (2008), *available at* http://commcns.org/XfofFi. The global market for cloud computing is predicted to increase from approximately $41 billion in 2011 to $241 billion in 2020. Jennifer Valentino-DeVries, *More Predictions on the Huge Growth of 'Cloud Computing,'* WALL ST. J. BLOGS (Apr. 21, 2011, 11:19 AM), http://commcns.org/VNkxXN.

Coinciding with this swell of cloud computing, consumers and their governmental representatives have become increasingly sensitive to how their personal information is protected by cloud providers.[6] In response, many countries have taken steps to protect consumer data through legislative action.[7] In October 1995, the European Union enacted Directive 95/46/EC in an effort to harmonize data protection laws across the E.U. Member States.[8] Renowned as one of the most comprehensive data protection laws enacted in any country, the E.U. Directive has served as a model for legislation in many non-European countries.[9]

The United States, however, has never passed a comprehensive regulation on data privacy, instead relying on a sectorial approach to privacy regulation.[10] In part due to the lack of a comprehensive data privacy law, European cloud customers have become reluctant to do business with cloud service providers based in the United States. In fact, according to a recent survey, seventy percent of Europeans are concerned with the security of their online data, due in large part to a mistrust of U.S. privacy protections.[11] European consumers cite the USA PATRIOT Act ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," or "PATRIOT Act"),[12] which was enacted after the terrorist attacks of September 11, 2001, to grant the federal government more authority to obtain information about suspected terrorists, as emblematic of the United States' loose stance on

---

[6] Alex Palmer, *Report: 90% Of Consumers Worry About Online Privacy*, DIRECT MARKETING NEWS (Feb. 10, 2012), http://commcns.org/Uyu2ru (finding that "[n]inety percent of U.S. adults worry about online privacy, while 41% do not trust most companies with their personal data); Quentin Hardy & Nicole Perlroth, *Companies Raise Concerns Over Google Drive's Privacy Protections*, N.Y. TIMES (Apr. 25, 2012, 3:41 PM), http://commcns.org/VawFDy.

[7] *See generally* Oliver Brettle & Nicholas Greenacre, White & Case LLP, Countries At A Glance—Data Privacy (2007), http://commcns.org/Xil28D (summarizing the relevant law and practice of each country in the areas of collection, processing, and transfer of personal data).

[8] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1329 (2000). *See generally* Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://commcns.org/Vt8zBt.

[9] Reidenberg, *supra* note 8, at 1329 n.66 (listing Chile and Argentina as examples of Latin American countries adopting European-style laws).

[10] Jean Slemmons Stratford & Juri Stratford, *Data Protection and Privacy in the United States and Europe*, 22 IASSIST Q. 17-18 (1998), *available at* http://commcns.org/W3rSlx.

[11] Jennifer Baker, *European Distrust of US Data Security Creates Market For Local Cloud Service: Europeans Worried About the US Patriot Act Prefer to Keep Their Data in the EU*, COMPUTERWORLD.COM (Dec. 2, 2011, 7:55 AM), http://commcns.org/XHME9f.

[12] *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles and sections of the U.S. Code).

data privacy.[13] The potential for U.S. data surveillance has prompted some European consumers to abandon contract negotiations with U.S.-based cloud providers.[14]

The situation became increasingly tense after Microsoft declined to guarantee that U.S. authorities would not access European customer data under the PATRIOT Act.[15] Since then, some European-based cloud providers have seen consumer concern over the PATRIOT Act as way to stir up sentiment for European protectionism in cloud services. Recently, European-based cloud providers have marketed their services as a way to circumvent American jurisdiction and protect consumer data from the reaches of the PATRIOT Act.[16] France Telecom went as far as to proclaim that, "if all the data enterprises were going to be under control of the U.S., it's not really good for the future of the European people."[17]

European government officials are echoing the private sector's distrust of American privacy laws, and some have urged European companies to avoid U.S.-based cloud providers. For example, Dutch Minister of Safety and Justice, Ivo Opstelten, cited the PATRIOT Act as a reason to exclude U.S. cloud providers from bidding on Dutch government contracts.[18] Moreover, a member of the Dutch parliament stated that, "data from Dutch citizens that is managed by

---

[13] *See* Amy Freeland, *Data Privacy Protection Discrepancies Could Hamper U.S. Cloud Provider Growth In Europe*, NTTCOM.TV (Jan. 30, 2012), http://commcns.org/Wkmo3r.

[14] *See* Sean Gallagher, *PATRIOT Act and Privacy Laws Take a Bite Out of US Cloud Business*, ARS TECHNICA (Dec. 8, 2011, 8:49 AM), http://commcns.org/XHMIFU (reporting that Patriot Act fears squashed BAE Systems' plans to adopt Microsoft Office 365, a cloud-based version of the Microsoft Suite).

[15] Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent* 1 (Queen Mary Univ. of London, Working Paper No. 74, 2011), *available at* http://commcns.org/XHMJcX. When asked whether Microsoft could "guarantee that EU-stored data, held in EU based datacenters, will not leave the European Economic Area under any circumstances — even under a request by the Patriot Act," Gordon Frazer, the managing director of Microsoft UK, replied that "Microsoft cannot provide those guarantees. Neither can any other company." Zack Wittaker, *Microsoft Admits Patriot Act Can Access EU-Based Cloud Data*, ZDNET (June 28, 2011, 8:10 AM), http://commcns.org/WbW4Zr.

[16] *See, e.g.*, Jennifer Baker, *Europe Cloud Vendors Cleaning Up With Data Protection Fears*, TECHWORLD (Dec. 5, 2011, 10:14 AM), http://commcns.org/W3s2JH ("[T]wo Swedish companies, Severalnines and City Network, have begun promoting their newly merged service as 'a safe haven from the reaches of the US Patriot Act.'"); Cornelius Rahn, *Deutsche Telekom Wants 'German Cloud' to Shield Data From U.S.*, BLOOMBERG.COM (Sept. 13, 2011, 6:00 PM), http://commcns.org/W9KX2f (quoting German cloud operator, T-Systems' CEO, Reinhard Clemens, in his attempt to lure customers by stating that "[a] German cloud would be a safe cloud.").

[17] Barb Darrow, *Buckle Up for A New Wave of Cloud Protectionism*, GIGAOM (Jan. 17, 2012, 6:40 AM), http://commcns.org/XHMMp7.

[18] Alan Charles Raul, *RAUL: Preventing Digital Trade War in the Cloud*, THE WASHINGTON TIMES (Oct. 28, 2011), http://commcns.org/UyuGVV.

the government should exclusively be stored within Dutch borders using Dutch companies."[19] European lawmakers characterize the PATRIOT Act as a mechanism for U.S. authorities to gain access to E.U. consumer data, and have taken a hard stance against it.

Despite support for European protectionism in the cloud, it is not clear that choosing a European-based cloud service provider will protect a consumer's information from the reaches of the PATRIOT Act. As this paper will show, the reach of the PATRIOT Act is wide and potentially encompasses European cloud providers that operate entirely within the European Union. Furthermore, an analysis of the European Privacy Directive reveals that it provides little, if any, greater protection for consumer information in the national security context. In response to the numerous calls for European customers to abandon U.S.-based could providers, this paper will critically analyze the legal grounds for the claim that the PATRIOT Act is reason to promote European protectionism in cloud services. Part II of this paper provides a general overview of the technical and commercial architecture of cloud computing. Part III discusses the PATRIOT Act and its extraterritorial applications to European-based cloud providers. Part IV examines the current framework and scope of the European Privacy Directive. Part V concludes with a discussion on the merits of European protectionism in the cloud and recommends an approach to achieve a coordinated system to protect the security interests of consumers.

II. WHAT IS CLOUD COMPUTING?

Understanding how the cloud operates is essential to appreciate the complex jurisdictional issues that arise in cloud computing. Some consider the cloud to have "supra-territoriality" because of the extent of its network capabilities, the multiple layers of service models offered, and the ability for data to be transferred to remote locations—often without the consumer's knowledge.[20] This section will detail the architecture of the cloud, and examine the reasons why special jurisdictional issues may arise for data stored in the cloud.

In essence, cloud computing is remote computing with software and data-

---

[19] *Id. cf.* Viviane Reding, Vice-President, European Comm'n, Speech at the Second Annual European Data Protection and Privacy Conference: The Future of Data Protection and Transatlantic Cooperation (Dec. 6, 2011), *available at* http://commcns.org/WkmRCw ("We need free flow of data between our continents. And it doesn't make much sense for us to retreat from each other.").

[20] Alan Charles Raul, *Real Harmony in Cloud Computing Between U.S., EU Closer Than You Think*, DAILY REP. FOR EXECUTIVES (BNA), July 26, 2011, *available at* http://commcns.org/YcoI1F; *see also* Bharath Chandrasekhar, *What is Cloudbursting?*, TREND CLOUD SECURITY BLOG (Mar. 15, 2011), http://commcns.org/11CW0HX (noting that new innovations allow data to "seamlessly" transfer to another location to meet heightened demand).

bases accessed through the Internet.[21] The services are generally paid for by the amount that they are used, but in some cases there may also be a modest subscription fee, or it may be free for use and paid for through advertising.[22] The main concept of cloud computing is that IT services, which were traditionally carried out on user-owned hardware and software, are outsourced to cloud provider machines and software that the consumer rents from the cloud provider.[23] Consumers usually choose to outsource IT services to the cloud because it reduces IT overhead, allows for greater flexibility, and reduces the total cost of a user's computing practices.[24] A cloud has five essential characteristics, is categorized into three different service models, and is deployed in four different models.[25]

A. Five Essential Characteristics of the Cloud

As defined by the National Institute of Standards and Technology ("NIST"), a cloud includes: (1) on-demand self-service, (2) broad network access, (3) resource pooling, (4) rapid elasticity, and (5) measured service.[26] First, through on-demand self-service, a consumer can "unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider."[27] In other words, a consumer is able to purchase resources on an as-needed basis.[28] In the context of the cloud, a consumer may purchase more infrastructure capacity within minutes, compared to the weeks or months it would take to increase capacity through building a traditional in-house IT architecture.[29]

Second, cloud computing enables broad network access. That is, resources stored on the cloud are available on any computing device, regardless of platform (*e.g.*, desktop, laptop, mobile phone, or tablet), from any Internet-

---

21 Harshbarger, *supra* note 1, at 231.

22 Miranda Mowbray, *The Fog Over the Grimpen Mire: Cloud Computing and the Law*, 6 SCRIPTED 129, 133 (2009).

23 *Id.*

24 Mladen A. Vouk, *Cloud Computing – Issues, Research and Implementations*, 16 J. Computing & Info. Tech. 235 (2008).

25 Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing, in* RECOMMENDATIONS OF THE NAT'L INST. OF STANDARDS & TECH., at 2 (Nat'l Inst. of Standards & Tech., Special Publication Ser. No. 800-145, 2011), *available at* http://commcns.org/10CUHcR.

26 *Id.*

27 *Id.*

28 Thomas W. Shinder, *Private Cloud Security Challenges – On Demand Self Service*, MICROSOFT TECHNET WIKI, http://commcns.org/Vt9DFm (last updated Jan. 17, 2012, 11:55 AM).

29 *Id.*

connected location.[30] Thus, a consumer is able to transition from platform to platform without having to transfer data from one device to another. The versatility broad network access provides is attractive to many consumers, and is often the most recognized feature of cloud computing.[31]

Resource pooling, the cloud's third characteristic, refers to the fact that computing resources available on the cloud (*e.g.*, storage, software, and network bandwidth) are shared by multiple consumers simultaneously. This type of architecture is called a "multi-tenant model" because multiple consumers (tenants) occupy the same set of resources.[32] Resource pooling is beneficial to the cloud provider because it allows data to reassign tenants to different locations in the cloud in order to optimize resource usage. However, this also means that the consumer generally has no control over—or knowledge of—the exact location of his or her data.[33] This type of arrangement could lead to consumer confusion and may subject consumer data to other jurisdictions without the consumer's knowledge.

Closely related to resource-pooling is rapid elasticity of services. A cloud's rapid elasticity allows a consumer to easily purchase more computing resources in any quantity, at any time.[34] If a consumer anticipates an increased demand for cloud services, they can simply purchase more capacity from the cloud provider. This also enables a consumer to scale back those services if demand eventually decreases.[35] For service providers, this means that capabilities must expand or contract based on corresponding customer demand.[36]

Finally, "[c]loud systems automatically control and optimize resource use by leveraging a metering capability," typically on a pay-per-use or charge-per-use basis, in a way that is appropriate for the type of service.[37] In this respect, the cloud provider acts much like a utility service—it measures the amount of resources that the consumer uses and charges the consumer accordingly.[38]

---

30 Mell & Grance, *supra* note 25, at 2.

31 *Id.* (describing broad access networks as an "essential characteristic").

32 *Id.*

33 *Id.*

34 Mell & Grance, *supra* note 25, at 2.

35 Clint Boulton, *Forrester's Advice to CFOs: Embrace Cloud Computing to Cut Costs*, EWEEK.COM (Oct. 31, 2008), http://commcns.org/U4Udac (describing this scalability as a "by-the-drink" payment plan). The value of the Cloud's ability to elastically provision resources arises from the fact that businesses must worry about both excess and insufficient resources; the former is costly and inefficient, while the latter poses serious risks, such as lost business opportunities. Joe Weinman, *Cloudonomics: A Rigorous Approach to Cloud Benefit Quantification*, 14 J. SOFTWARE TECH. 10, 10, 14-15 (2011), *available at* http://commcns.org/XHN4we.

36 Mell & Grance, *supra* note 25, at 2.

37 *Id.* at 2 & n.1. Some examples of services requiring different levels of metering capabilities include "storage, processing, bandwidth, and active user accounts." *Id.* at 2.

38 Weinman, *supra* note 35, at 10, 14.

B. Cloud Architecture and Service Models

Cloud computing architecture consists of three layers: infrastructure (hardware), platform (operating systems), and application (software run by the user).[39] These three layers can be conceptualized as stacked upon each other, with the application layer working on top of the platform, which in turn works on top of the infrastructure.[40] Corresponding with each of these architecture layers are three different service models: Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Software as a Service ("SaaS").[41] As explained below, each service model gives the consumer a different level of functionality and control.

With IaaS, the consumer purchases infrastructure services from the cloud provider, but manages the layer on top of the infrastructure itself.[42] Consumers of IaaS generally include application owners and others who need access to virtual servers and cloud storage.[43] The PaaS model offers the consumer a development platform in addition to the services provided with IaaS, and gives the consumer the capability of deploying his or her own applications "using programming languages, libraries, services, and tools" that the PaaS provider supports.[44] Consumers of PaaS are generally application owners who outsource the platform necessary to run these applications.[45] Finally, the SaaS model offers the costumer the full application service for the cloud service provider.[46]

---

[39] Grace Walker, *Cloud Computing Fundamentals, A Different Way to Deliver Computer Resources*, IBM (Dec. 17, 2010), http://commcns.org/W9LcdL; *see also* Mell & Grance, *supra* note 25, at 2 & n.2 (abstractly summarizing the Cloud's framework).

[40] Kate Craig-Wood, *IAAS vs. PAAS vs. SAAS Definition*, KATE'S COMMENT (May 18, 2010, 4:39 PM), http://commcns.org/Vt9TEu (using graphic material to better explain the relationships between IaaS, PaaS, and IaaS).

[41] Lee Badger et al., *Cloud Computing Synopsis and Recommendations*, *in* RECOMMENDATIONS OF THE NAT'L INST. OF STANDARDS & TECH., at 2-1, 2-2 (Nat'l Inst. of Standards & Tech., Special Publication Ser. No. 800-146, 2012); *see also* Bart Czernicki, *IaaS, PaaS and SaaS Terms Clearly Explained and Defined*, SILVERLIGHT HACK (Feb. 27, 2011, 1:23 PM), http://commcns.org/U4Ugmx (using two simple, but very helpful, diagrams to explain IaaS, PaaS, and SaaS).

[42] Badger, *supra* note 41, at 2-2; *see also* Czernicki, *supra* note 41 (noting that examples of IaaS include Windows Azure, RackSpace, and SoftLayer); *see generally* Craig-Wood, *supra* note 40.

[43] Bill Loeffler et al., *Reference Architecture for Private Cloud: What is Infrastructure as a Service*, MICROSOFT TECHNET WIKI, http://commcns.org/Vt9XUz (last updated Mar. 22, 2012, 4:39 PM) (discussing, in the "Comparison of Cloud Service Models" diagram, the consumer-base for SaaS, PaaS, and IaaS).

[44] Mell & Grance, *supra* note 25, at 2-3.

[45] Loeffler et al., *supra* note 43 (discussing, in the "Comparison of Cloud Service Models" diagram, the consumer-base for PaaS); *see also* Craig-Wood, *supra* note 40 (diagraming the set-up of the service layers and listing, as examples, the following providers of infrastructure software: Java, Windows, ORACLE and Google apps).

[46] Mell & Grance, *supra* note 25, at 2; Czernicki, *supra* note 41 (describing SaaS as the layer giving "business functionality"); *see generally* Loeffler et al., *supra* note 43 (providing

This is the layer with which consumers are most familiar, as it runs on-demand applications such as Gmail, Facebook, and Dropbox.[47]

The tiered structure of the cloud means that the services provided to the end user usually involve layers of providers of which the consumer is unaware.[48] For instance, while consumers of the file-storage service DropBox see it as a SaaS provider, DropBox, which relies on Amazon's infrastructure, considers Amazon an IaaS provider.[49] In this way, companies have the discretion to specialize in one level of cloud service, which ultimately provides better products for the customer. However, this fragmented approach to cloud services results in a lack of direct consumer-control over data. Thus, consumers may remain uncertain of the jurisdiction that governs the protection of their data.

C. Deployment Models

The final way that cloud services are delineated is by deployment models: private, public, community, or hybrid. In a private cloud, the infrastructure is for the exclusive use of a single organization with multiple consumers or business units.[50] The infrastructure may be owned and operated by the organization itself, a third party, or some combination of the two; the servers may be on-site or outsourced to a hosting company.[51]

In a public cloud, the infrastructure is open for use by the general public or a large industry group and is owned and operated off-site by a cloud service provider.[52] Including systems such as the Google App Engine, Microsoft Windows Azure, and Amazon EC2, this is the type of deployment with which consumers are most familiar.[53]

In a community cloud, the cloud infrastructure is shared by several organizations with a common interest or objective (*e.g.*, mission, security requirements,

---

a useful table listing the typical SaaS provider's consumer-base, as well as the services it provides).

47 Walker, *supra* note 39 (noting Gmail, Google Calendar, and Google Docs as examples of SaaS providers). W Kuan Hon & Christopher Millard, *Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4*, 9 SCRIPTED 25, 29 & n.14 (2012), *available at* http://commcns.org/Vaxf4d (last visited Nov. 10, 2012) (identifying DropBox and Facebook as prominent examples of a SaaS).

48 Hon & Millard, *supra* note 47, at 29.

49 *Id.*

50 Mell & Grance, *supra* note 25, at 3.

51 Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 170 (2011-2012).

52 John Soma et al., *Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services*, 16 J. TECH. L. & POL'Y 193, 198 (2011).

53 Cade Metz, *Say Hello to Windows Azure, the World's Most Misunderstood Cloud*, WIRED ENTERPRISE (Apr. 27, 2012, 6:30 AM), http://commcns.org/W3suaE.

policy, or compliance considerations).[54] However, like a private cloud, it may exist on or off-site, managed by the organizations themselves or outsourced to a third party.[55] The community cloud model is particularly useful for sharing services with multiple departments or agencies of the same entity. For instance, Microsoft is developing a community cloud for use by U.S. federal, state, and local governments.[56]

Finally, a hybrid cloud is composed of two or more cloud models—private, community, or public—that remain separate and unique entities. Despite their apparent separation, these entities are bound together by standardized or propriety technology that enables data and applications to be transferred between the two when necessary.[57] This type of data portability is called "cloud bursting," and allows a cloud system to utilize resources from a connected system when demand requires.

The boundless nature of the cloud has the potential to subject consumer data to multiple jurisdictions. The multi-tenant approach that allows for greater economies of scale and lower prices, also leads to the potential for consumer data to be stored and subject to jurisdictions that consumers are not even aware. Furthermore, the choosing a public deployment model in which resources are shared can limit the consumer's control over his or her data. The next section will examine the provisions of the PATRIOT Act that related to data security issues, then discuss the extent to which the PATRIOT Act can apply extraterritorially given the global nature of the cloud.

III. THE PATRIOT ACT

In response to the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon, the United States Congress passed the PATRIOT Act.[58] The PATRIOT Act was reauthorized in 2006,[59] with the addition of some privacy protections,[60] and again in 2010.[61] The primary objective of the PA-

54 Mell & Grance, *supra* note 25, at 3.

55 Soma et al., *supra* note 52, at 198.

56 Rutrell Yasin, *Microsoft Building a Government Community Cloud*, GCN (Mar. 2, 2012), http://commcns.org/10CV1Zk.

57 Mell & Grance, *supra* note 25, at 3.

58 *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

59 Extension of Sunset of Certain Provisions of the USA PATRIOT Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 109-160, 119 Stat. 2957 (2005).

60 USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006) (codified at 50 U.S.C. § 1861(d)–(g) (2006)) (clarifying that individuals who receive FISA orders can challenge nondisclosure requirements, and that individuals who receive NSLs are not required to disclose the name of their attorney).

TRIOT Act was to provide federal officials with more discretion to intersect domestic and foreign communications, "both for law enforcement and foreign intelligence gathering purposes."[62] Although the PATRIOT Act did not create any new procedural mechanism for U.S. law enforcement officers to obtain information, it expanded the scope of certain discovery mechanisms that were already available.[63] Today, two discovery mechanisms are relevant to obtaining data on the cloud: Foreign Intelligence Surveillance Court Orders ("FISA Orders")[64] and National Security Letters ("NSLs").[65]

A. Expanded Authority to Issue Foreign Intelligence Surveillance Court Orders

Prior to the PATRIOT Act, the Foreign Intelligence Surveillance Act ("FISA") permitted the Federal Bureau of Investigation ("FBI") to apply to a special court, the Foreign Intelligence Surveillance Court, to obtain business records for the primary purpose of gathering information on foreign powers or an agent of a foreign power.[66] FISA Orders were granted in *ex parte* proceedings, with only the FBI presenting evidence to the court.[67] Records were originally limited to car rentals, hotels, storage lockers, and common-carrier records.[68]

Section 215 of the PATRIOT Act expanded the scope of FISA Orders in three important respects. First, it expanded the type of documents that could be obtained to include "any tangible thing[] (including books, records, papers, documents and other items) for an investigation to protect against international

---

[61] USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 Extensions, Pub. L. No. 111-141, 124 Stat. 37 (2010) (codified at 50 U.S.C. §§ 1801, 1805, 1861, 1862 (2010)). This act extends the use of roving wiretaps, searches for business records, and conducting surveillance of individuals suspected of terrorist-related activities not linked to terrorist groups. *Obama Signs Last-Minute Patriot Act Extension*, FOXNEWS.COM (May 27, 2011), http://commcns.org/Sb1Koc.

[62] CHARLES DOYLE, CONG. RESEARCH SERV., RL31377, THE USA PATRIOT ACT: A LEGAL ANALYSIS 1 (2002), *available at* http://commcns.org/Sb1QML.

[63] *See* Alex C. Lakatos, *The USA PATRIOT Act and the Privacy of Data Stored in the Cloud*, MAYER BROWN (Jan. 18, 2012), http://commcns.org/UTSUIF.

[64] EDWARD C. LIU, CONG. RESEARCH SERV., R40138, AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) EXTENDED UNTIL JUNE 1, 2015, at 1, 4 (2011), *available at* http://commcns.org/U4Us5k.

[65] *See* Lakatos, *supra* note 63 (defining a "National Security Letter" as "a form of administrative subpoena that the FBI and other US government agencies can use to obtain certain records and data pertaining to various types of government investigations").

[66] Peter P. Swire, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA PATRIOT Act: Surveillance Law: Reshaping the Framework: The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1329 (2004); *see also* Lakatos, *supra* note 63.

[67] Lakatos, *supra* note 63.

[68] *Id.*

terrorism and clandestine intelligence activities."[69] This includes data stored in the cloud.[70] Second, Section 215 of the PATRIOT Act included a "gag" provision, which prevents a party receiving a FISA order from disclosing that fact.[71] Thus, in practical application, a cloud service provider would be prohibited from informing its customers that it shared the customer's data with the FBI.[72] Third, the legal standard to obtain the order was changed, eliminating the need for any particularized showing.[73] Rather, the FBI need only "specify that the records concerned are sought for an authorized investigation...to protect against international terrorism or clandestine intelligence activities."[74] In practical effect, this change means that FISA orders can apply to someone who is neither the target of the investigation, nor an agent of a foreign power.[75] In relation to the cloud, Section 215 would allow an entire database to be subject to a FISA order as long as there is "an authorized investigation."[76]

Under the USA PATRIOT Act Improvement and Reauthorization Act of 2005, Congress addressed some of these concerns under Section 215 by adding a provision that allows the recipient of a FISA order to oppose it before the FISA court and to contest the gag order after one year. Despite these changes, many providers and consumers alike remain troubled by this provision.[77]

B. Expanded Authority to Issue National Security Letters

NSLs are administrative subpoenas issued by a federal agency that require the production of information held by third parties,[78] such as financial institutions, consumer reporting agencies, and wire or electronic service providers, such as cloud providers.[79] NSLs are particularly worrisome because they do not require judicial oversight.[80] Additionally, they include a "gag" provision that prohibits the third party from disclosing that it received an NSL.[81] Prior to the

---

69 *See* 50 U.S.C. § 1861(a) (2006).

70 Lakatos, *supra* note 63.

71 *Id.*

72 *Id.*

73 Swire, *supra* note 66, at 1331.

74 50 U.S.C. § 1861(b)(2) (2006).

75 Swire, *supra* note 66, at 1329.

76 *Id.*

77 Lakatos, *supra* note 63.

78 *The Permanent Provisions of the PATRIOT Act: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 13 (2011) (statement of Todd Hinnen, Acting Assistant Att'y Gen. for National Security) [hereinafter *2011 PATRIOT Act Hearing*].

79 Lakatos, *supra* note 63.

80 Swire, *supra* note 66, at 1331.

81 *2011 PATRIOT Act Hearing*, 13 (statement of Todd Hinnen, Acting Assistant Att'y Gen. for National Security).

PATRIOT Act, NSLs granted the FBI authority to subscriber information from telephone companies and Internet Service Providers and account information from banks and credit reporting agencies.[82] Section 505 of the PATRIOT Act, Removing Obstacles to Investigating Terrorism, dramatically expanded the scope of NSLs.

Similar to the expansion of FISA orders under Section 215, Section 505 amended the standard of proof that is required to issue NSLs. Previously, NSLs were not issued without specific and articulable facts demonstrating that the information sought pertained to a foreign power or to an agent of a foreign power.[83] Under the PATRIOT Act, however, NSL issuance requires only that the material be relevant to a national security investigation. Not surprisingly, the use of NSLs began to dramatically increase after their scope was expanded,[84] from 8,500 NSLs in 2000 to between 39,000 and 49,000 per year from 2003 to 2006.[85] In 2010, the FBI made 24,287 NSL requests compared to only 14,788 in 2009.[86]

Additionally, Section 205 expanded the number of officials that are authorized to issue NSLs. First, it granted all fifty-six FBI field offices with the authority to make NSL requests. Second, it granted any government agency, not just the FBI, with the authority to obtain information from a consumer-reporting agency in connection with international terrorism or intelligence activities.[87] This expansion of officials authorized to issue NSLs has led to increased concerns over the general lack of privacy safeguards under the PATRIOT Act.

Concerns over the lack of privacy safeguards under the PATRIOT Act were addressed in federal district court[88] and ultimately led to amendments of the Act in 2005,[89] and again in 2006.[90] In *Doe v. Ashcroft*, the court addressed the Act's failure to provide for any judicial review of the FBI's decisions to issues

---

82 Swire, *supra* note 66, at 1332.

83 *2011 PATRIOT Act Hearing*, 15 (statement of Todd Hinnen, Acting Assistant. Att'y Gen. for National Security).

84 Lakatos, *supra* note 63.

85 AM. CIVIL LIBERTIES UNION, RECLAIMING PATRIOTISM: A CALL TO RECONSIDER THE PATRIOT ACT 12 (2009), *available at* http://commcns.org/Wko2ly.

86 Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the June 8, 2011, Hearing Before the S. Comm. on the Judiciary Regarding The President's Request to Extend the Service of Dir. Robert Mueller of the FBI Until 2013, at 1 (Aug. 15, 2011), *available at* http://commcns.org/Vaxmgf.

87 *See* 15 U.S.C. §§ 1681u(a)–(b), 1681v (2006); Lakatos, *supra* note 63.

88 *See* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *see also* Doe v. Gonzales, 386 F. Supp. 2d 66, 78-82 (D. Conn. 2005).

89 USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 115, 116, 120 Stat. 192, 211-17 (2006).

90 USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006).

NSLs.[91] The Southern District of New York held that "the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violate[d] the Fourth Amendment, and that the ["gag" order] provision of 18 U.S.C. § 2709(c) violate[d] the First Amendment."[92] In *Doe v. Gonzales*, the Southern District of New York addressed the Act's failure to provide for any procedure to challenge a "gag" order.[93] The Court ruled that the "gag" order provision was unconstitutional because it violated both the First and Fourth Amendments.[94]

As amended, the PATRIOT Act includes a judicial enforcement mechanism and a judicial review procedure for requests and nondisclosure requirements.[95] The Act clearly states that the nondisclosure requirements do not preclude a recipient from consulting an attorney,[96] provides a process to modify or set aside the nondisclosure requirement,[97] expands congressional oversight,[98] and provides for an Inspector General's audit of their use.[99] The most notable of these changes is the right to judicial review of NSLs, which gives recipients the right to petition a federal court for an order modifying or setting aside the NSL and federal judges the authority to alter compliance if it would be unreasonable, oppressive, or otherwise unlawful.

C. Extraterritorial Application of the PATRIOT Act

In order to assess claims that refraining from using U.S.-based cloud service providers will protect European consumers from the reach of the PATRIOT Act, the territorially scope of the PATRIOT Act must be analyzed. Specifically, this involves examining the extent to which U.S. authorities can enforce the PATRIOT Act extraterritorially in order to force companies operating within the European Union to transfer data over to the U.S. government. There are two mechanisms by which U.S. authorities can extend the reach of the PATRIOT Act to European-based cloud providers. First, the United States can subpoena business records from any company, including cloud providers, so long as (1) they have personal jurisdiction over the entity, using the "minimum

---

91 *See Ashcroft*, 334 F. Supp. 2d 471; *see also Gonzales*, 386 F. Supp. 2d at 78-82; Lakatos, *supra* note 63.

92 *Ashcroft*, 334 F. Supp. 2d at 526-27.

93 *Gonzales*, 386 F. Supp. 2d at 78-82.

94 USA PATRIOT Improvement and Reauthorization Act of 2005 §§ 115-116; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.

95 18 U.S.C. § 3511 (2006).

96 12 U.S.C. § 3414(a)(3)(A) (2006); 15 U.S.C. §§ 1681v(c)(1), 1681u(d)(1) (2006); 18 U.S.C. § 2709(c)(1) (2006); 50 U.S.C. § 436(b)(1) (2006).

97 18 U.S.C. § 3511(b).

98 USA PATRIOT Improvement and Reauthorization Act of 2005 § 115.

99 18 U.S.C. § 2709.

contacts" standard, and (2) the entity is in "possession, custody, or control" of the data, regardless of the data's location.[100] Secondly, cloud providers operating in the European Union without any connection to the United States may still be obligated to disclose their customers' data under Mutual Legal Assistance Treaties ("MLATs") or on voluntary assistance by member E.U. states.

1. Enforcing the PATRIOT Act through Personal Jurisdiction

Personal jurisdiction stemming from "minimum contacts" is based on the Due Process Clause as expressed in the Supreme Court decision *International Shoe v. Washington.*[101] Essentially, any company incorporated in the United States or corporation that has its principle place of business in the United States is subject to U.S. jurisdiction. In addition, any company that has "continuous and systematic" contacts with the United States may also be subject to U.S. jurisdiction.[102] It is important to note that the personal jurisdiction considerations do not consider the "minimum contacts" of the consumer whose information is being sought by the government. Rather, it is the cloud provider's jurisdictional contacts that are relevant in determining whether the information may be seized under the PATRIOT Act.[103] Because the cloud provider has "control" of their consumer's data, it is capable of being seized through the provider by the government.[104]

Once a cloud provider is served with a subpoena, the provider must produce all documents that are in its "possession, custody, or control."[105] This includes all data that may be in the "possession, custody, or control" of a branch or subsidiary of a U.S.-based provider that is located anywhere in the world.[106] To determine a party's level of control over the relevant documents, the court considers the closeness of the relationship between the entities.[107] In *In re Uranium Antitrust Litigation*, the U.S. District Court of the Northern District of Illinois, Eastern Division, ruled that it had the authority to compel production of docu-

---

[100] Stuart D. Levi, *Cloud Computing: Understanding Security and Jurisdictional Issues*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM, LLP (Apr. 3, 2012), *available at* http://commcns.org/VtaHZX (follow the "Download PDF" hyperlink).

[101] Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).

[102] Goodyear Dunlop Tires Operations, S.A. v. Brown, 131 S. Ct. 2846, 2851 (2011) (holding that a defendant must be "essentially at home" in order to exercise personal jurisdiction for "continuous and systematic" contacts).

[103] Levi, *supra* note 100.

[104] *Id.*

[105] FED. R. CIV. P. 34(a)(1); Lakatos, *supra* note 63.

[106] Lakatos, *supra* note 63.

[107] John Whelan & Sally-Anne Hinfey, *No Cloud Over the PATRIOT Act*, A & L GOODBODY (A&L Goodbody, Dublin, Ir.), March 2012, ¶ 3.3, *available at* http://commcns.org/WLsqIX.

ments located abroad if the court had personal jurisdiction over the defendants and the defendants had control over the documents, despite conflicting foreign law.[108] The court found that a U.S. court can order an American parent corporation to produce the documents of its foreign subsidiary when the "corporation has power, either directly or indirectly, through another corporation or series of corporations, to elect a majority of the directors of another corporation . . . ."[109]

However, the court noted that this power is discretionary and should be informed by three factors: "1) the importance of the policies underlying the U.S. statute which forms the basis for the plaintiff['s] claims; 2) the importance of the requested documents in illuminating key elements of the claims; and 3) the degree of flexibility in the foreign nation's application of its nondisclosure laws."[110] Additionally, U.S. courts can refuse to exercise its power in a way that would violate foreign law, consistent with the principles of comity.[111] While the court found some leeway for judicial discretion in compelling foreign entities to provide data to U.S. authorities, the essence of the PATRIOT Act – combatting terrorism – raises the expectation that most courts will consider the requested information of such high importance that they will enforce the United States' right to compel the production of documents.[112]

For cloud service providers, this means that the U.S. government will be able to serve FISA orders, NSLs, warrants or subpoenas compelling them to provide their customers' data if the company is incorporated in the United States, has an office or branch in the United States, or conducts "continuous or systematic" business within the United States, regardless of the actual location of the stored data.[113] Due to the wide scope of jurisdictional reach, a consumer's choice to purchase a European-based cloud provider is not enough to ensure that data is beyond the reach of the PATRIOT Act.

2. Enforcing the PATRIOT Act through Mutual Legal Assistance Treaties

While it might appear that European companies are able to secure their data from the reach of U.S. jurisdiction by either declining to do business in Amer-

---

[108] *In re* Uranium Antitrust Litig., 480 F. Supp. 1138, 1148 (N.D. Ill. 1979) (involving an antitrust action where the plaintiffs moved for production of documents but three foreign statues, enacted for the express purpose of frustrating jurisdiction by U.S. courts, prohibited disclosure of the documents).

[109] *Id.* at 1144-5.

[110] *Id.* at 1148 (summarizing Societe Internationale v. Rogers, 357 U.S. 197 (1958)).

[111] *Cf. id.*

[112] *See, e.g.*, U.S. DEP'T OF JUSTICE, FACT SHEET: SHIFTING FROM PROSECUTION TO PREVENTION, REDESIGNING DOJ TO PREVENT FUTURE ACTS OF TERRORISM (2002), http://commcns.org/WbXao0 ("[d]efending our nation and defending the citizens of America against terrorist attacks is our first and overriding priority").

[113] Lakatos, *supra* note 63.

ica or declining to do business with American customers, that is not likely the case. The United States and most European governments have entered into bilateral Mutual Legal Assistance Treaties ("MLATs") under which both governments commit to work together in criminal investigations in order to access information where they would otherwise not have jurisdiction.[114] Most MLATs declare that the countries will provide one another with "the widest measure of mutual assistance in investigations or proceedings in respect of criminal offenses."[115]

In 2003, the United States and European Union updated their Mutual Legal Assistance Treaty to include a provision addressing data protection.[116] The original MLATs did not speak directly to data privacy issues, but did allow for denials for requests of information based on public policy grounds.[117] The U.S.-U.K., U.S.-German, and U.S.-France MLATs, for instance, all contain the provision that requests could be denied if it would "impair [the requested country's] sovereignty, security, or other essential interests or would be contrary to important public policy."[118] The changes in the 2003 agreement were "meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases."[119] The comments to this provision specifically prohibit a country from refusing to comply with a request because the nations have different systems for protecting data privacy or because the requesting nation lacks a specified data protection authority.[120] Therefore, U.S. requests concerning terrorism investigations are rarely denied.[121]

European consumers are certainly justified in their concern about the privacy of their data as a result of the PATRIOT Act, but choosing an E.U.-based cloud service provider will not ensure that their data is beyond its reach. Due to the wide jurisdictional scope that American courts afford the PATRIOT Act, in

---

[114] Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 98 AM. J. INT'L L. 579, 596 (2004); Lakatos, *supra* note 63.

[115] *See* Treaty on Mutual Legal Assistance in Criminal Matters Between the United States of America and France, U.S.-Fr., Dec. 10, 1998, Art. 1, T.I.A.S. No. 13010, *available at* http://commcns.org/WkokJf [hereinafter France MLAT]; *see also* Lakatos, *supra* note 64.

[116] Agreement on Mutual Legal Assistance Between the European Union and the United States of America, U.S.-E.U., art. 9, June 29, 2003, 2003 O.J. (L 181/34) (EC), *available at* http://commcns.org/UyvQko [hereinafter E.U. MLAT].

[117] *See, e.g.*, Lakatos, *supra* note 63.

[118] Treaty Between the United States of America and the United Kingdom and Northern Ireland on Mutual Legal Assistance on Criminal Matters, U.S.-U.K., art. 3, Jan. 6, 1994, T.I.A.S. No. 96-1202, *available at* http://commcns.org/13Jvyw0; France MLAT, *supra* note 116, art. 6; Supplementary Treaty to the Treaty of October 14, 2003 Between the United States of America and Germany on Mutual Legal Assistance, U.S.-Ger., art. 6, Apr. 18, 2006, T.I.A.S. No. 09-1018.1, *available at* http://commcns.org/Vtbeex.

[119] E.U. MLAT, *supra* note 116, at n.9.

[120] *Id.*

[121] *See, e.g.*, Lakatos, *supra* note 63.

addition to the MLAT agreements between the United States and the members of the European Union, it is unlikely that cloud providers will be able to evade the scope of U.S. investigations.[122] Applying U.S. personal jurisdiction doctrine, U.S.-based companies and subsidiaries, as well as foreign companies that do substantial business in the United States, satisfy the "minimum contacts" test and thus may be ordered to produce any information in their "possession, custody, or control."[123] Even if a company circumvents U.S. jurisdictional authority, law enforcement will be able to obtain information through the Mutual Legal Assistance Treaties with the E.U. member states.[124]

IV. THE EUROPEAN DATA PROTECTION DIRECTIVE

Another factor to consider when deciding whether it is worthwhile to boycott American cloud service providers is the extent to which European laws protect consumer data in similar circumstances. In 1995, the European Commission issued "Directive 95/46 of the European Parliament and Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data".[125] The Directive was established in order to provide a regulatory framework that guarantees the free and secure movement of personal data across the national borders of E.U. member countries, while setting a security standard for the storage, transmission, and processing of personal data.[126] As with all E.U. Directives that become law, the Directive was implemented in each of the twenty-seven member states' own national law, through legislation enacted locally.[127]

---

[122] *Id.*

[123] *Id.*; *see also* Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (outlining the "minimum contacts" requirement for exercising personal jurisdiction over an individual or corporation); FED. R. CIV. P. 34(a)(1) (providing that an individual or corporation subject to U.S. jurisdiction and served with a valid subpoena must produce any documents within its "possession, custody, or control").

[124] The EU-MLAT comments explain that this provision was "meant to ensure that refusal of assistance on data protection grounds may be involved only in exceptional cases[,]" and, as a result U.S. MLAT requests "are seldom denied for data protection reasons." Lakatos, *supra* note 63. *See, e.g.*, James K. Knapp, *Mutual Legal Assistance Treaties as a Way To Pierce Bank Secrecy* 20 CASE W. RES. J. INT'L L. 405 (1988); Julian M. Joshua, Peter D. Camesasca & Youngjin Jung, *Extradition and Mutual Legal Assistance Treaties: Cartel Enforcement's Global Reach,* 75 ANTITRUST L.J. 353 (2008-2009).

[125] Council Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281/31) (EU), *available at* http://commcns.org/W3sPdv [hereinafter Data Protection Directive].

[126] *EU Data Protection Directive,* ELECTRONIC PRIVACY INFORMATION CENTER, http://commcns.org/VtblXi (last visited Nov. 10, 2012).

[127] *Application of EU Law, What are EU directives?,* EUROPEAN COMM'N, http://commcns.org/XHNHG2 (last updated June 25, 2012) (explaining that "EU directives

A. General Provisions

The Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject')" that may be identifiable "directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."[128] It distinguishes between data controllers, those who "determined the purposes and means of the processing of personal data"[129] and data processors, who "process[] personal data on behalf of the controller."[130] "Processing" is all inclusive, and pertains to "any operation or set of operations which is performed upon personal data... ."[131]

The Directive places obligations on data "controllers" who either operate within the European Economic Area ("EEA"), who are "established" in the EEA, or who "make[] use of" equipment located in the EEA.[132] The data controller owes a duty to the data subject when the personal data is collected directly from the person.[133] Additionally, the controller must implement appropriate technical and organizational measures against unauthorized processing.[134]

Of particular importance to cloud providers, the Directive prohibits the transfer of personal data outside of the EEA to a third country unless the third country "ensures an adequate level of protection."[135] Because the cloud operates on a borderless network,[136] this places a substantial burden on the data controller to ensure that consumer data is not transferred outside of the EEA or, if data is transferred outside the EEA, that the third country has been deemed to have an adequate level of protection.[137] Currently, only a few countries outside

---

lay down certain end results that must be achieved in every Member State . . . but [national authorities] are free to decide how to do so"). Because the Directive had to be implemented on a local basis, there are some inconsistences in application of the Directive. Hon & Millard, *supra* note 48, at 28-29. This paper will focus on generally accepted applications of the Directive.

128 Data Protection Directive, *supra* note 125, art. 2(a).

129 *Id.*, art. 2(d).

130 *Id.*, art. 2(e).

131 *Id.*, art. 2(b) (listing such actions as "collection, recording, organization, storage, electronic storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"); *see also Cloud Computing and EU Data Protection Law*, COMPUTERWORLDUK.COM (Sept. 28, 2011, 4:00 PM), *available at* http://commcns.org/U4USZk.

132 *Id.*, art. 4.

133 *Id.*, art. 4.

134 *Id.*

135 *Id.*, art. 25(1).

136 Mell & Grance, *supra* note 25, at 2.

137 Paul M. Schwartz, *Data Protection Law and The European Union's Directive: European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV.

of the European Union have been declared by the European Commission to have the requisite level of protections to satisfy the Directive.[138] The United States is not one of these countries deemed to have an adequate level of protection.[139] This status has not been given to the United States because of the reach of the PATRIOT Act and its lack of a comprehensive privacy regulation or governmental agency devoted to privacy, and lack of governmental agency devoted to privacy.[140]

B. Safe Harbors

To help bridge the differences between the U.S. approach to privacy and that of the E.U., the European Commission adopted Decision 520/2000/EC on July 26, 2000, which recognized certain safe harbors for transferring data into the United States.[141] The U.S. Department of Commerce worked with the European Commission to develop U.S.-specific safe harbors, whereby U.S. organizations that promise to adhere to seven principles of privacy protection may transfer data with European companies.[142] To qualify for the safe harbor, the U.S. organization must (1) adhere to seven Safe Harbor principles that ensure U.S.-based companies provide adequate privacy protection;[143] and (2) publicly announce its compliance through certification letters filed annually with the Department of Commerce or its designee.[144]

C. Exemptions to Data Protection Directive

While a major goal of the Directive is to provide comprehensive protection of personal data, drafters attempted to strike a "balance between the right to be

---

471, 483-84 (1995).

[138] These countries include, Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, and Jersey. Hon & Millard, *supra* note 47, at 26, 31.

[139] Charles Batchelor, *Privacy: US and EU Clash on Confidentiality*, FINANCIAL TIMES (May 22, 2012, 4:56 PM), http://commcns.org/VaxCMo.

[140] *Id.*

[141] Commission Decision 2000/520/EC, of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7, 10-12 (EC), *available at* http://commcns.org/Xfrr3y.

[142] *See Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000), http://commcns.org/Ycplsa.

[143] These seven principles include: (1) notice; (2) choice; (3) access; (4) onward transfer; (5) security; (6) data integrity; and (7) enforcement. James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145, 151-52 (2001).

[144] *Id.* at 151.

let alone and the legitimate interests of a society."[145] In this vein, the Directive's scope does not cover a number of uses of personal data, including: 1) all activity falling not within the scope of "community law", such as national security, defense, public safety, economic or financial interests of the state, and criminal proceedings;[146] 2) activities conducted solely for research;[147] 3) activities "solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression;"[148] and 4) transfers of data to third countries without adequate privacy laws if that transfer is done with the data subject's consent, is pursuant to a contract, is required for a legitimate public interest, or if the transferor adduces adequate safeguards by the transferee.[149]

Most European countries have utilized the Directive's exception for "community law" and have passed laws specifically restricting data protection for national security reasons. For example, the Netherland's national data protection law states that, "this Act does not apply to the processing of personal data . . . by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act [or] . . . for the purposes of implementing police tasks."[150] The U.K. has similarly made personal data "exempt from any of the provisions of . . . the data protection principles . . . if the exemption from that provision is required for the purpose of safeguarding national security."[151] Spanish law provides that data protection "shall not apply to the collection of data when informing the data subject would affect national defense, public safety or the prosecution or criminal offences."[152]

The Directive affords E.U. consumers with substantial rights and protections in their personal data, but the national security exemptions to the law allow data to be unprotected in the same instances when the PATRIOT Act applies. Critics who point to the PATRIOT Act as an example of the United States falling short of E.U. data privacy protections fail to recognize that the European Privacy Directive does not apply when national security is at risk, or even in

---

[145] Stephen A. Oxman, Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?, 24 B.C. INT'L & COMP. L. REV. 191, 192-93 (2000) (quoting Ulrich U. Wuermeling, Harmonisation of European Union Privacy Law, 14 J. MARSHALL J. COMPUTER & INFO. L. 411, 414 (1996)).

[146] Council Directive 95/46, art. 3(2), 1995 O.J. (L 281) 31, 39 (EC).

[147] *Id.* at 42.

[148] *Id.* at 41.

[149] *See id.* at 46.

[150] Wet Bescherming Persoonsgegevens [Dutch Data Protection Act] art. 2(2)(b-c), Stb. 2000, p. 302 *available at* http://commcns.org/11CWY78 (unofficial translation).

[151] Data Protection Act, 1998, c. 29, art. 28(1) (U.K.), *available at* http://commcns.org/XHNQte.

[152] LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal art. 24, (B.O.E. 1999, 15), *available at* http://commcns.org/Sb2YQz (unofficial translation).

the prosecution of criminal offenses. In fact, when national security considerations are invoked, a consumer's data, whether American or European, is not protected from the reaches of government surveillance.

V. CONCLUSION

A critical examination of United States and European Union law indicates that simply avoiding U.S.-based cloud service providers based on concerns about the PATRIOT Act will not necessarily protect consumer data. Due to the wide jurisdictional scope of the PATRIOT Act and MLATs with European nations, merely selecting a European-based cloud provider does not guarantee that consumer data will be beyond the reaches of the PATRIOT Act. If the cloud provider is a subsidiary of a U.S.-based company, has a data center located in the United States, or has "continuous and systematic" contacts with the United States, it will be within the jurisdictional reach of the PATRIOT Act. Even if a consumer chooses an E.U.-based provider that is outside the scope of the PATRIOT Act, the United States will still potentially have access to the data pursuant to MLAT treaties with its European allies.

The potential for intrusive governmental surveillance of personal data is not exclusive to the United States. Both the United States and the European Union allow the government substantial leeway in obtaining consumer information. In particular, the PATRIOT Act authorizes access to data for national security reasons, such as "international terrorism and clandestine intelligence activities."[153] Similarly, the E.U. Directive makes an exception for "community law," which includes national security, defense, public safety, economic or financial interests of the state, and criminal proceedings,[154] and authorizes "[m]ember States [to] adopt legislative measures to restrict the scope of the obligation and rights . . . when such a restriction constitutes a necessary measure to safeguard . . . national security."[155] Thus, an E.U. consumer's data is subject to government confiscation for national security reasons regardless of the location of the cloud service provider.

---

[153] USA PATRIOT Act of 2001, Pub. L. No. 107-56, §505, 115 Stat. 365 (2001); *see also* Lakatos, *supra* note 63.

[154] *See* Oxman, *supra* note 149, at 191 (citing Ulrich U. Wuermeling, *Harmonisation of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411, 414 (1996)); *see also* Council Directive 95/46/EC, rec. 43, 1995 O.J. (L 281/31) (EU) (stating that "restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example national security...").

[155] Council Directive 95/46/EC, art. 13.