The Sedona Conference Journal

Volume 13 2012

Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act

Steven C. Bennett, M. James Daley & Natascha Gerlach

Recommended Citation: Steven C. Bennett, M. James Daley & Natascha Gerlach, *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act*, 13 SEDONA CONF. J. 235 (2012).

For this and additional publications see:
https://thesedonaconference.org/publications

STORM CLOUDS GATHERING FOR CROSS-BORDER DISCOVERY AND DATA PRIVACY: CLOUD COMPUTING MEETS THE U.S.A. PATRIOT ACT

Steven C. Bennett
Jones Day
New York City, NY

M. James Daley
Daley & Fey
Overland Park, KS

*Natascha Gerlach**
Cleary Gottlieb Steen & Hamilton
Brussels, Belgium

Last June, a Microsoft executive noted at a launch of Microsoft 365 in London that U.S.-based Cloud Computing[1] providers could be compelled, notwithstanding the EU Data Protection Directive,[2] to secretly release personal data of EU citizens pursuant to a National Security Letter (NSL) under the U.S.A. Patriot Act ("Patriot Act"), even if that data is stored on servers physically located within the EU region. These statements sparked a more vigorous global debate regarding the conflict between cross-border discovery and data privacy.[3] This article examines the controversy surrounding the extraterritorial reach of the Patriot Act to global "Cloud Computing" providers.[4] In particular, it considers whether, and to what extent, the Patriot Act[5] may apply to Cloud Computing providers, and how this may impact the cross-border discovery/disclosure and data privacy conflict. The article also suggests some best practices to help mitigate risk in this context.

---

* Steven C. Bennett, Esq. is a partner at Jones Day and Chair of the Firm's E-Discovery Committee. M. James Daley Esq., CIPP/US is partner and co-founder of Daley & Fey, a boutique law firm devoted to global E-Discovery and data privacy issues. Natascha Gerlach, Esq. is a Senior Staff Attorney for Litigation and E-Discovery at Cleary Gottlieb Steen & Hamilton. Jerilyn Laskie, a summer associate at Jones Day and Dylan Murray, Esq. and Zach Hemenway, Esq., Counsel at Daley & Fey, and Pia Caruana, Paralegal at Cleary Gottlieb Steen & Hamilton assisted in the preparation of this article. The views expressed are solely those of the authors, and should not be attributed to the authors' firms, their clients, or to The Sedona Conference®, or any of its Working Groups.

1 Cloud computing is defined as "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." Peter Mell, "The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology," *NIST Special Publication*, 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; *see also* W. Kuan Hon, Christopher Millard, Ian Walden, "The Problem of 'Personal Data' in Cloud Computing – What Information Is Regulated?," 2001, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/11/1995*.

3 *See* Jennifer Baker, "EU upset by Microsoft warning on U.S. access to EU Cloud," *Computerworld*, July 5, 2011, http://www.computerworld.com/s/article/9218167. Jeff Bullwinkle, Director of Legal and Corporate Affairs at Microsoft Australia, stated: "In a limited number of circumstances, Microsoft may need to disclose data without your prior consent, including as needed to satisfy legal requirements, or to protect the rights or property of Microsoft." *See also* Zach Whittaker, "European companies 'need confidence' over Patriot Act concerns," September 1, 2011, http://www.zdnet.com/blog/btl/european-companies-need-confidence-over-patriot-act-concerns/56878.

4 Deputy Assistant Attorney General Bruce Schwartz is reported to have commented: "The Patriot Act really in this context is a red herring. It didn't work a fundamental change in how we approach the issues of stored data." Kenneth Corbin, "Foreign Cloud Privacy Issues Dismissed by U.S. Officials," *CIO Magazine*, January 19, 2012, http://www.cio.com/article/698312/Foreign_Cloud_Privacy_Issues_Dismissed_by_U.S._Officials.

THE DRIVE TOWARD CLOUD COMPUTING

Although "Cloud Computing" is an evolving technology paradigm, it essentially involves remote hosting and Internet access to various combinations of computer hardware, software, and data.[6] The drive toward Cloud Computing is fueled by economics – the ability to reduce the increasingly high cost of in-house information technology ("IT") systems and services.[7] According to an independent study by the Pew Research Center, 71% of technology experts and stakeholders expect that by 2020, most people will access software applications online and share and access information through the use of remote Cloud Computing networks, rather than individual, personal computers.[8] And according to independent technology consultant Gartner, the Cloud Computing industry is expected to grow from annual revenues of $68.3b in 2010 to $148.8b in 2014.[9] By leveraging and sharing large IT infrastructures, platforms, software, and data storage centers, Cloud Computing can, by conservative estimates, reduce by 25 to 30 percent the "all-in" costs of traditional IT services.[10] It also provides small and medium size organizations without sufficient budget with a reliable, available, and affordable IT option. In this sense, Cloud Computing can use economies of scale to "even the playing field" between small and large business. Cloud Computing allows companies to outsource IT service, cutting expenses for equipment, labor, training, security, and other costs associated with maintaining an on-site data services.[11]

Cloud Computing also significantly alters the data security risk landscape in one important respect – now, the obligation for data security and the protection of personal information stored in the cloud squarely rests upon the shoulders of the cloud service provider.[12] Cloud service providers may be located and do business anywhere in the world, thus subjecting them to the laws of the many jurisdictions. The Patriot Act is one such law, which may create serious complications for cloud service providers and those who choose to use them.

APPLICATION OF THE PATRIOT ACT

The Patriot Act essentially aggregates a variety of U.S. statutory provisions and procedures related to law enforcement, surveillance, and privacy protection, including the

---

5 Pub. L. No. 107-56, 115 Stat. 272 (2001). The full title of the Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A. PATRIOT ACT) Act of 2001."

6 *See* Jared A. Harshbarger, "Cloud Computing Providers and Data Security Laws: Building Trust With United States Companies," *16 J. Tech. L. & Pol'y* (2011): 229, 231; *see also* National Institute of Standards and Technology, "Cloud Computing Synopsis and Recommendations" (May 2012): § 2 (discussing the essential characteristics, service models, and deployment models with respect to cloud computing).

7 For additional background regarding the impact of new technologies on cross-border discovery and data privacy conflicts, see also M. James Daley, "Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure and Data Privacy," *11 Sedona Conf. J. 121* (Fall 2011).

8 "Cloud Computing," "Cloud Recovery," "Elon University Cloud Survey," Pew Research Center, June 16, 2010, http://cloudrecovery.info/2010/06/16/responses-to-a-tension-pair-on-the-likely-future-of-cloud-computing/.

9 *See* Cornelius Rahn, "Deutsche Telekom Wants 'German Cloud' to Shield Data From U.S.," Bloomberg, September14, 2011, http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.

10 *See* Afzal Bari, "Federal Cloud Computing and Data Center Consolidation," a Bloomberg study, *http://www.actgov.org/events/managementofchange/MOC2011/MOC%202011%20Documents%20and%20Presentations/federal%20cloud%20computing%20and%20data%20center%20consolidation.pdf ;see also, e.g.,* Booz Allen Hamilton, "The Economics of Cloud Computing," http://www.boozallen.com/media/file/Economics-of-Cloud-Computing-fact-sheet.pdf.

11 Harshbarger, *16 J. Tech. L. & Pol'y*: 232-33; for a discussion of these benefits and the expected growth of cloud computing, *see* Janna Quitney Anderson and Lee Rainie, "The Future of Cloud Computing," Pew Internet & American Life Project, http://pewresearch.org (almost three quarters of surveyed technology experts and stakeholders believed that by 2020 most people will access software applications online and as a result they will "live mostly in the cloud").

12 Harshbarger, *16 J. Tech. L. & Poly*: 235; *see also* National Institute of Standards and Technology, "Cloud Computing Synopsis and Recommendations" (May 2012): § 8.5 (discussing generally cloud computing information security issues); ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security" (November 2009); "Who's Responsible for Personal Data in Cloud Computing?," May 23, 2011, http://blogs.computerworlduk.com/cloud-vision/2011/05/whos-responsible-for-personal-data-in-cloud-computing/index.htm.

Foreign Intelligence Act of 1978 ("FISA"), the Electronic Communications Privacy Act of 1986 ("ECPA"), the Money Laundering Control Act of 1986, and the Bank Secrecy Act ("BSA").[13] In broad terms, the Act permits and amplifies the application to terrorism of techniques commonly used to fight organized crime. One of the most controversial changes of The Patriot Act is to expand the availability and scope of National Security Letters ("NSLs"). NSLs are essentially subpoenas that that can require service providers to provide non-content information (*e.g.*, telephone numbers) about a subscriber's transactions, without a court order. The Patriot Act makes NSLs more widely available by removing the limitation that they relate to non-content information (*e.g.*, telephone numbers) pertaining to a foreign power or its agents. In addition, the Patriot Act also makes NSLs more readily available by removing the time-consuming requirement that they be approved in advance by senior FBI agents.

Even more alarming to EU Regulators, a secret U.S. court can issue FISA letters to compel the production of the actual content of communications. And FISA orders typically are accompanied by a gag order, prohibiting the recipient from any statement about the FISA order. Although the Patriot Act is intended to enhance the ability of U.S. law enforcement agencies to obtain information relevant to terrorist activities, the ability to obtain electronic communication data, including personal data, without any notice to customers or data controllers constitutes a significant change in the law.[14]

Specifically, the Act provides that the contents of electronic communications held by a "remote computing service" may be disclosed "without notice to the subscriber or customer" if the government obtains a warrant using procedures described in the Federal Rules of Criminal Procedure by a "court with jurisdiction over the offense under investigation."[15] To obtain such information, the government must provide a "court of competent jurisdiction" with "specific and particular facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication" are "relevant and material to an ongoing criminal investigation."[16] A court of "competent jurisdiction" includes a court in the district where the offense is under investigation, or a district where the wire or electronic communication service is located.[17] Alternatively, a limited amount of record information, such as subscriber names and addresses, telephone numbers, credit card and bank account numbers, and billing records, can be obtained using an administrative, grand jury, or trial court subpoena.[18]

FISA orders apply "without geographic limitation,"[19] a change the Department of Justice requested.[20] Thus, courts are authorized "to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located."[21] The Act permits "computer taps" as well, involving the installation of devices to record information kept by a computer regarding routing, addressing, and signaling.[22]

13 Congressional Record: October 11, 2001 (Senate) Page S10547-S10630.
14 *See* 18 U.S.C. Sec. 2703(a), (d).
15 *See* 18. U.S.C. Sec. 2703(a).
16 *See* 18 U.S.C. Sec. 2703(d).
17 18 U.S.C. Sec. 3127(2) (definitions).
18 18 U.S.C. Sec. 2703(c)(1)(C).
19 18 U.S.C. Sec. 2703.
20 Charles Doyle, "The USA Patriot Act: A Legal Analysis 6 n.12," *CRS Rep.No. RL31377* (2002).
21 *Id.* at 7 n.14.
22 Janine Anthony Bowen, "Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations," *1043 PLI/Pat* (2011): 375, 383.

U.S. APPROACH TO JURISDICTION OVER INFORMATION

Criminal Discovery Procedures

The Patriot Act does not modify the "possession, custody, or control" standard for discovery set forth in the Federal Rules of Criminal Procedure.[23] Nor does it expressly address the extraterritorial effect of warrant provisions of U.S. criminal procedure. And due to the broad judicial interpretations of the "possession, custody or control" standard in the Federal Rules of Criminal Procedure, the U.S. government could (in theory) obtain information from a U.S.-based cloud service provider – including records related to foreign customers (perhaps including customers in EU countries – without any notice to those customers.

Civil Discovery Procedures

Information stored electronically has become one of the most important sources of discoverable material, and because many use electronic devices such as computers and smart phones for both business and personal reasons, U.S. discovery rules often sweep in documents that include personal data.[24] Under long-standing principles of U.S. law, a U.S. court with jurisdiction over a company may compel the company to produce information in the company's "possession, custody, or control."[25] Thus, under U.S. law, even if a court cannot exercise jurisdiction over an absent party, it may nevertheless compel access to information in the hands of the absent party where another party, subject to the court's jurisdiction has, through the absent party, "possession, custody, or control" of the information.[26]

Thus, "the test for production of documents is control, not locations."[27] Further, U.S. courts have interpreted the concept of control "broadly as the legal right, authority, or practical ability to obtain the materials sought upon demand."[28] Using this analysis on "possession, custody, or control," U.S. courts have, on many occasions, ordered the production of information in the possession of foreign entities, where the court has jurisdiction over a related entity in a U.S. proceeding.[29]

APPLICATION OF THE EU DATA PROTECTION DIRECTIVE TO CLOUD SERVICE PROVIDERS

A cloud service provider's production of data stored outside the U.S., or relating to foreign citizens pursuant to the Patriot Act, may subject the provider to legal sanctions

---

23 Fed. R. Crim. P. 16(b)(1).

24 Alan Charles Raul et al., "Reconciling European Data Privacy Concerns with US Discovery Rules: Conflict and Comity," *Global Competition Litigation Review*, no. 3, (2009): 119, 120.

25 *See* Federal Rules of Criminal Procedure ("Fed. R. Crim. P.") 16(a)(1)(E), 16(b)(1)(A), 17(c)(1) (subpoenas); Federal Rules of Civil Procedure ("Fed. R. Civ. P.") 34, 45 (subpoenas).

26 *See Dietrich v. Bauer*, 2000 U.S. Dist. LEXIS 11729 (S.D.N.Y. 2000) (citing *Afros S/P.A. c. Krauss-Maffei Corp.*, 113 F.R.D. 127, 129 (D. Del. 1986) ("personal jurisdiction and 'control' of documents are distinct issues in that [the] court can compel discovery of documents in [the] 'control' of a party although in 'possession' of a person over whom there is no personal jurisdiction.").

27 *Dietrich v. Bauer*, 2000 WL 1171132 at *2 (S.D.N.Y. Aug. 16, 2000) (quoting *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983)).

28 *See Bank of New York v. Meridien Biao Bank Tanzania*, 171 F.R.D. 135, 146 (S.D.N.Y. 1977); *see also Goodman v, Praxair Servs. Inc.*, 632 F. Supp. 494, 516 n.11 (D. Md. 2009); *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007); *Asset Value Fund, Ltd. V. The Care Group, Inc.*, 1997 U.S. Dist. LEXIS 19768 at 9 (S.D.N.Y. 1997).

29 *See, e.g.*, *Gucci Amer., Inc. v. Curveal Fashion*, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010) (ordering party discovery from Malaysia); *AccessData Corp v. ALSTE Techs.*, 2010 WL 318477, at *7 (D. Utah Jan. 21, 2010) (ordering party discovery from Germany); *In Re Cargo Shipping Srvs. Antitrust Litig.*, 2010 WL 1189341, at *5 (E.D.N.Y. Mar. 29, 2010) (ordering party discovery from France).

under the laws of other nations.[30] In particular, as briefly summarized below with respect to the EU, compliance with such demands may violate laws governing privacy protection for personal data.

The EU Data Protection Directive

Directive 95/46/EC of the European Parliament and Council,[31] commonly called the Data Protection Directive ("Directive"), essentially requires all EU member states to adopt legislation to enforce certain essential data protection principles. These data protection principles include:

1. Notice (providing data subjects with notice when their data is collected);
2. Purpose (data should only be used for the purpose stated);
3. Consent (data should not be disclosed without the data subject's consent);
4. Security (data should be kept secure from potential abuses);
5. Disclosure (data subjects should be informed as to their data);
6. Access (data subjects must be able to access and correct their data; and
7. Accountability (data controllers are accountable for ensuring adherence with data protection principles).

The Directive forbids transfer of personal data of a data subject, without notice and consent, to a government or entity that has not committed to follow EU data protection principles. Currently, only a few countries are considered to have "adequate" data protection under the Directive, with the U.S. notably excluded.[32]

Thus, for example, in 2006 the European Court of Justice, applying the Directive, struck down a negotiated agreement between the European Council and U.S. Customs to share information regarding the names of passengers involved in trans-Atlantic flights, where prior arrangements had not been made to ensure adequate protection of the information.[33]

The EU Data Directive

Article 4 of the Directive, as adopted by individual EU member states, governs the application of the Directive to Cloud Computing. The EU Article 29 Data Protection Working Party, an independent advisory body established pursuant to Article 29 of the Directive, has issued a specific opinion on Cloud Computing.[34] In its opinion,

30 *See* "Data Protection, the Law and You: The Cloud of Unknowing," and the "'Personal Data'" Problem," April, 13, 2011, http://blogs.computerworlduk.com/cloud-vision/2011/04/data-protection-the-law-and-you-1/index.htm.
31 Available at www.eur-lex.europa.eu; *see generally* Peter Hustinx, "Data Protection and Cloud Computing Under EU Law" (speech given at Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010).
32 *See* "European Commission Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries," "List of Countries Covered by a Commission Adequacy Finding Decision," www.ec.europa.eu/justice/.
33 *See* "Article 29 Data Protection Working Party, Opinion 5/2006 on the ruling by the European Court of Justice," adopted June 14, 2006, www.ec.europa.eu/justice (in light of ruling "any transfer of passenger data to the U.S. would be without a legal basis in European law").
34 Opinion 8/2010 on "Applicable Law," December 16, 2010, www.ec.europa.eu/justice.

the Article 20 Working Party noted that, in circumstances involving Cloud Computing, "[t]he exact place where data are located is not always known," but it is "sufficient" for EU jurisdiction to enforce privacy standards that a data "controller," such as a cloud service user/customer, "carries out processing in the context of an establishment within the EU." Thus, "[i]f the company [customer] uses the service in the context of the activities of its establishment in the EU," then in the opinion of the Article 29 Working Party, the Directive will apply, and "[t]he company should make sure that the service provides for adequate data protection safeguards [.]"[35]

Article 4 and the scope of the national laws have in the past been applied quite broadly,[36] and some Data Protection Authorities ("DPAs") have even conducted enforcement audits in countries outside the EU.[37] In this light, a Patriot Act request for information regarding EU data subjects, whether from a U.S.-based cloud service provider or an EU-based provider, would appear to implicate the Directive. The Directive states that processing of personal information is justified only where necessary because of a "legal obligation," or where the processing aligns with the data controller's "legitimate interests." Because U.S. discovery has not generally been regarded as either a "legal obligation" or "legitimate interest" in the EU, the Directive limits the collection, processing, and transfer of personal information to satisfy U.S. litigation requirements.[38] This restriction could create a conflict between obligations under U.S. and EU law. The easiest way to comply with the EU Data Protection Directive – ensuring that personal data stays within the EU – is not always achievable due to the very nature of Cloud Computing.[39]

Companies do, however, have other options to comply with the Directive.[40]

Safe Harbor

A cloud provider can subscribe to the International Safe Harbor Certification program.[41] The Safe Harbor program was developed by the U.S. Department of Commerce, and approved by the European Commission, and consists of a standard set of privacy principles to which companies must agree in order to create and ensure an "adequate level of protection" of personal data, consistent with the Directive.[42] U.S. companies that publicly certify compliance with the principles are therefore allowed to pass data from the EU to the U.S., although if data is stored outside the EU or the U.S., the Safe Harbor becomes ineffective.[43] The problem, of course, is that although the Safe

35 *Id.* at 21; *see also* "Cloud Computing and EU Data Protection Law, Part One: Understanding the International Issues," September 28, 2011, http://blogs.computerworlduk.com/cloud-vision/2011/09/cloud-computing-and-eu-data-protection-law/index.htm.

36 *See* excellent analysis by C. Kuner, Submission to the "Consultation on the Commission's comprehensive approach on personal data protection in the European Union," http://ec.europa.eu/justice/news/consulting_public/0006/contributions/citizens/kuner_christopher_en.pdf, p. 5 ff., with a call to narrow the focus of the future Art. 4.

37 *See, e.g.*, Agencia Española de Protección de Datos, "Report on International Data Transfers: Ex officio Sectorial Inspection of Spain-Colombia at Call Centres," July 2007, https://www.agpd.es/portalweb/jornadas/transferencias_internacionales_datos/common/pdfs/report_Inter_data_transfers_colombia_en.pdf.

38 Raul, *supra* note 18, at 120.

39 *See generally* Andrew Geyer and Melinda McLellan, contributors, "Strategies for Evaluating Cloud Computing Agreements," *Bloomberg Law Reports* (2011).

40 *See* "Cloud Computing and the EU Data Protection Law, Part Two: On International Transfers of Personal Data," April 23, 2012, http://blogs.computerworlduk.com/cloud-vision/2012/04/cloud-computing-and-eu-data-protection-law-part-two/index.htm.

41 "Safe Harbor Overview," http://www.export.gov/safeharbor/eg_main_018236.asp (last updated April 27, 2011, 2:31 PM).

42 Paul Lanois, "Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy," *9 Nw. J. Tech. & Intell. Prop.* (2010): 29, 48. Commentators have pointed to similar certifications for providers who meet HIPAA security requirements and have suggested a similar program be created for cloud providers. *See* "The Cloud Also Rises: PHI Security in the Era of Cloud Computing," http://www2.idexpertscorp.com.

43 Lanois, *9 Nw. J. Tech. & Intell. Prop.*: 48.

Harbor program permits compliance with the EU directive, once the data is in the U.S., it may become subject to government inspection pursuant to the Patriot Act.[44]

Outside of the question of onward transfer, the Düsseldorfer Kreis, a group of top DPAs for the non-public sector in Germany, adopted a resolution on April 29, 2010 setting even stricter requirements for cross-border transfer of data under Safe Harbor, by placing the burden of Safe Harbor certification and compliance onto the transferring company.[45] If the new and stricter requirements cannot be met, the use of standard contractual terms is recommended.[46]

Standard Contractual Clauses

Alternatively a cloud provider located in a country other than the U.S. can sign standard forms of contracts, commonly known as Standard Contractual Clauses (SCC). So far the European Commission has issued two separate sets of SCCs, one for controllers (Set II[47]) and another for processors.[48] These must be used in the precise form approved by the European Commission to provide an adequate level of protection enabling data transfer between a data exporter in the EU and a data importer outside the EU. These SCCs should in theory suffice for an automatic compliance with EU standards, but the strict scrutiny and varied outcome among the Member States[49] make them a difficult tool. The SCCs are independent of the principle contract between the consumer and the cloud provider. While the use of (un-amended) SCCs automatically ensures compliance with EU standards, and can therefore be considered advantageous to the customer, they also bare a risk for the service provider of enforceability beyond the basic contract.[50]

Despite the difficulties surrounding SCCs, cloud providers located in countries that have not been white-listed by the European Commission and which are not Safe Harbor certified might consider making use of SCCs to comply with the requirements of the Directive.

Binding Corporate Rules

Entities with global subsidiaries have the additional option of setting up "binding corporate rules" (BCRs) for the purpose of sharing data within the group in compliance with European regulations. BCRs are a legally binding internal set of documents laying down the group's intended safeguards to individuals whose personal data is transferred to a third country. The level of protection must be equal to that provided for by the Directive. Following internal agreement on BCRs, they are submitted to one national data protection

44 Zack Whittaker, "Why EU data needs 'protecting' from US Law," April 25, 2011, http://www.zdnet.com.
45 http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungDuesseldorferKreis/290410_SafeHarbor.html;jsessionid=2FE330DB52E8317B1FDBBE6DB2C5C445.1_cid136?nn=409242.
46 http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungDuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile.
47 The initial Set I was considered too restrictive and not used frequently.
48 Available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF and http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.
49 Certain countries require standard clauses to be filed and approved prior to the initial transfer, while other countries do not call for any additional formalities. In addition, difficulties in characterizing controllers and processors often lead to different classifications of one and the same compliance program. *See* Renzo Marchini, *Cloud Computing*, 74.
50 *See an extensive analysis in* Renzo Marchini, *Cloud Computing*, 75 and Christopher Kuner, *European Data Protection Law – Corporate Compliance and Regulation* (2007), 195 et seq.; concerning cloud computing contracts generally, *see* "Cloud Computing Contracts and Services: What's Really Happening?," March 17, 2011, http://blogs.computerworlduk.com/cloudvision/2011/03/cloud-computing-contracts-and-services-whats-really-happening/index.htm; *see also* Simon Bradshaw, Christopher Millard, and Ian Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services," September 1, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

regulator, who in turn coordinates the approval required by other national authorities.[51] In 2008 the Article 29 Working Party provided for a 'one-stop' shop mutual recognition scheme for BCR covering 19 member states, whereby approval by the leading national authority automatically brings about approval in the other member states.[52] Due to the currently high cost and complexity of this option, it is best suited for facilitating the transfer of data within large entities.

APPROACHES TO DATA PRIVACY IN OTHER JURISDICTIONS: CANADA AND AUSTRALIA

Aside from the EU, many countries have in place some kind of data protection regime, although the scope and effect of these regimes vary widely. Because Canada and Australia have been leaders in data protection legislation, particularly among non-EU countries, it is helpful to contrast them to the EU data protection framework.
Data protection in Canada is governed by the Personal Information Protection and Electronics Documents Act (PIPEDA). Unlike the EU approach, which focuses on the level of privacy protection given by law in other states, Canada focuses on the level of protection guaranteed by particular organizations. That is, organizations themselves are responsible for the information they transfer to third parties, regardless of whether those parties reside within Canada. The law thus encourages contracts between organizations, with the expectation that data service providers will demonstrate adequate methods of protecting personal information. In Canada, organizations must follow ten principles whenever they collect, use, or disclose personal information – as compared with the seven EU data protection principles set out above. These Canadian principles are:

1. Accountability (an organization is responsible for personal information under its control);

2. Identifying Purposes (purposes for which the information is collected must be identified before or at the time of collection);

3. Consent (knowledge and consent of the individual are required except where inappropriate);

4. Limiting Collection (information shall only be collected by fair and lawful means and collection must be limited to that which is necessary for the identified purposes);

5. Limiting Use, Disclosure, and Retention (information must not be used for any purpose other than that for which it was collected, except in the case of consent or as required by law);

6. Accuracy (information must be as accurate as necessary for purposes for which it is to be used);

7. Safeguards (information shall be protected by safeguards appropriate to its sensitivity);

51 Formal approval may at times be required by all 27 member states, depending on the size of the company. *See* Renzo Marchini, *Cloud Computing*, 81.

52 *See* Article 29 Working Party, "Working Document: Co-operation Procedure for Binding Corporate Rules," http://ec.europa.eu/justice/policies/privacy/binding_rules/procedure_en.htm. For more information on the coordination procedure see Christopher Kuner, *European Data Protection Law – Corporate Compliance and Regulation* (2007), 222 et seq.

8. Openness (policies and practices regarding an organization's management of information shall be readily available to individuals);

9. Individual Access (upon request, an individual shall have access to his or her information and have the ability to challenge the accuracy of the information and amend as necessary); and

10. Challenging Compliance (an individual retains the right to challenge compliance with the principles).[53]

In Australia, data protection is governed by the Privacy Act. The public sector is subject to 11 "Information Privacy Principles" and the private sector is subject to ten similar "National Privacy Principles." Australian entities may send information to third parties abroad under three circumstances: 1) the entity believes the recipient will uphold the principles; 2) the entity has consent from the data subject; or 3) the transfer is necessary to comply with contractual obligations."[54] The Privacy Act covers foreign entities operating in Australia as well as entities abroad that carry on business in Australia and collect or hold personal information about Australian citizens within Australia.[55]

As in the EU, these laws may create a conflict with the Patriot Act. That is, cloud service providers and other businesses operating in Canada and Australia may find it difficult to comply with national privacy laws when faced with a subpoena or court order for personal information issued pursuant to the Patriot Act.

U.S. APPROACH TO CONFLICTS OF LAW REGARDING DATA PROTECTION

The U.S. is party to a number of conventions and treaties that impact access to data, including Cloud Computing data, outside the U.S, for litigation and law enforcement purposes. These international agreements include the Hague Evidence Convention, the Agreement on Mutual Legal Assistance between the U.S. and E.U., and Treaties on Mutual Legal Assistance in Criminal Matters with a number of individual countries.[56]

In determining how to respond to requests under these agreements and treaties, EU member governments carefully weigh privacy concerns and often impose confidentiality restrictions to protect further dissemination of the information.[57] Many EU countries consider resort to such conventions and treaties to be the most appropriate – and sometime exclusive – way to seek access to data under the jurisdiction of a foreign sovereign.[58]

---

53 Leah E. Frazier, "Extraterritorial Enforcement of PIPEDA: A Multi-tiered Analysis," *36 Geo. Wash. Int'l L. Rev. 203* (2004): 206-08.

54 Russell Allen, "Compliance with Rules and Regulations Pertaining to Cross-Border Transfer of Personnel and Business Data: The Australian Perspective," *18 No. 1 Emp. & Indu. Rel. L.* 36 (2008): 37.

55 *Id.*

56 *See e.g.*, Agreement on Mutual Legal Assistance between the European Union and the U.S. (June 25, 2003) ("E.U.-U.S. Agreement"); U.S.-German Mutual Legal Assistance Treaty in Criminal Matters (October 14, 2003), Treaty Doc. 108-27, 108th Cong. 2d Sess.; Exec. Rept. 109-14, 109th Cong. 2d Sess.; Supplementary Treaty to the Mutual Legal Assistance Treaty in Criminal Matters (April 18, 2006), Treaty Doc. 109-13, 109th Cong. 2d Sess. Both German treaties entered into force on October 18, 2009.

57 For Example, Article 9 of the E.U.-U.S. Agreement, entitled "Limitations on use to protect personal and other data," provides that member states can impose conditions on use of information, but that "[g]eneric restrictions with respect to the legal standards of the requesting state for processing personal data may not be imposed by the requested State as a condition . . . to providing evidence or information."

58 *See e.g.* the Council of Europe's (COE) "Guidelines on Human Rights and the Fight Against Terrorism," July 11, 2002, http://www.coe.int/t/dlapil/cahdi/Source/Docs2002/H_2002_4E.pdf (laying down ground rules to be followed in fighting terrorism). *See also* the COE's Convention on Cybercrime of November 23, 2001, which aims at harmonizing national laws on cybercrime, improving national capabilities for investigating such crimes, and at increasing cooperation on investigations. A copy of the convention and an explanatory report are available at http://conventions.coe.int/Treaty/en/Treaties/html/185.htm and at http://conventions.coe.int/treaty/en/reports/html/185.html. *See also* Ian Walden, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent," November 14, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067.

It is also notable that the EU generally places the specific fundamental human right to privacy above general counter terrorism objectives.[59] While European DPAs have sometimes sought enforcement audits of data processors in other countries,[60] such audits require a specific legal basis, as well as the consent of the State concerned – in conformity with the fundamental sovereign rights of European states.[61]

The United States Supreme Court's Aérospatiale Doctrine

In contrast, the U.S. Supreme Court has held that U.S. courts may compel production of foreign evidence within the possession, custody, or control of an entity subject to U.S. jurisdiction, without following the procedures provided for in the Hague Evidence Convention. In *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, the Court held that use of the Convention is optional, not mandatory. The Supreme Court noted that the Hague Convention "doesn't modify the law of any contracting state [including the Federal Rules of Criminal and Civil Procedure], require any contracting state to use its procedures either in requesting evidence or in responding to requests, nor compel any contracting state to change its own evidence gathering procedures."[62] Despite this ruling, the Court in *Aérospatiale* noted the relevance of "comity" concerns in evaluating the scope and form of foreign discovery ordered by a U.S. court.[63] Applying this framework, U.S. courts have frequently held that significant U.S. government concerns may outweigh foreign interests in protection of private or confidential information.[64] Subpoenas and court orders have been issued even where disclosure is prohibited by law in the countries in which the information is located. The enforcement is not through a foreign court or treaty, but typically by a U.S. court through contempt proceedings, which can result in significant fines.[65] This threat of contempt penalties generally drives compliance and gives effect to subpoenas and orders outside the U.S., although other severe sanctions can include prosecution for obstruction of justice and dismissal of claims.[66]

Despite the general trend toward upholding U.S. interests against competing claims of foreign interests in privacy protection, some U.S. courts have streamlined, or even prohibited, U.S. disclosures in favor of protecting foreign interests.[67] In substance, the cases

59 As can be derived from ECtHR rulings post 9/11 (*see* Kim Lane Scheppele, *Other People's PATRIOT Act*, 139 et seq.) and the COE Convention and Guidelines (*see* footnote 58).

60 *See* Christopher Kuner, *Data Protection law and International Jurisdiction on the Internet (Part 2)*, 9 et seq.

61 *See supra* notes 53-55.

62 482 U.S. 522, 534 (1987).

63 *See Aerospatiale*, 482 U.S. 522, 544 (1987) (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 442(1)(c) (1987) (in deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the U.S. should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the U.S.; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the U.S., or compliance with the request would undermine important interests of the state where the information is located).

64 *See, e.g.*, *United States v. Bank of Nova Scotia*, 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983) (interest of the U.S. in upholding grand jury's power to investigate crime outweighed interests of the Cayman Island and Bahamas in bank secrecy laws): *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir.), *cert. denied*, 454 U.S. 1098 (1981) (strong U.S. interest in collecting taxes and prosecuting tax fraud by U.S. nationals outweighed Switzerland's interest in preserving business secrets of Swiss subsidiaries of American corporations); *In re United States v. First National City Bank*, 396 F.2d 897 (2d cir. 1968) (risk of civil liability in Germany was "speculative" where a federal grand jury in New York issued a subpoena to a New York bank requiring production of documents relating to transactions of its customers located both at its head office in New York and at its branch in Frankfurt, West Germany; importance of U.S. antitrust enforcement was greater than German interest in bank secrecy).

65 In *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984), the Bank failed to comply with a grand jury subpoena and was subsequently fined $1,825,00 for contempt of court.

66 Raul, *supra* note 18, at 120.

67 *See, e.g.*, *Salerno v. Lecia*, 1999 U.S. Dist. LEXIS 7169 (W.D.N.Y., Mar. 23, 1999) (production of severance package information and personnel files precluded by EU Privacy Directive 95/46/EC and by German Act on Data Protection); *Volkswagen AG, Relator v. Valdez*, 909 S.W.2d 900, 902 n.14 (Tex. 1995) (denying request to produce company telephone book, as protected by German Federal Data Protection Act, because production would undermine interests of Germany while no U.S. interest would be undermined if it was not produced, particularly where alternative methods of discovery of same information were available.

and commentators suggest that a careful "balancing" of interests should address these kinds of conflicts.[68] The Restatement (Third) of Foreign Relations, which outlines the U.S. approach, lists several factors that a court will consider in determining whether to order disclosure from abroad: the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the U.S., or compliance with the request would undermine important interests of the state where the information is located.[69] Because of the subjective nature of the factors involved, it may be difficult to predict whether a court will grant access to information held abroad; nevertheless, if the U.S. government claims an interest in preventing terrorist activity and makes an effort to limit the request, a U.S. court will probably grant access.

PRACTICAL IMPACT OF THE PATRIOT ACT

Because Patriot Act applications for warrants are not public, there is little available information regarding Patriot Act requests for U.S. based cloud service providers to disclose EU personal data. Even though the Patriot Act generally permits a party to challenge a subpoena or warrant for information in a court proceeding, research to date has failed to reveal any public challenges to Patriot Act requests on grounds of interference with the privacy of EU citizens.

Research reflects that from 2006-2009, 1755 "delayed-notice" search warrants were issued. Of those, 1619 (92%) were issued for drug-related investigations, 122 (about 7%) for fraud; and 15 (less than 1%) for terrorism related investigations.[70] These statistics suggest that the instances of U.S. government requests for EU citizen information pursuant to the Patriot Act are presumable quite rare.

Nevertheless, commentators generally agree that the "possession, custody, or control" standard, applied in the Patriot Act context, and with the imprimatur of the U.S. government's interest in fighting crime and terrorism, could be used to obtain such information.[71] In practical terms, where a company is subject to jurisdiction in the U.S., and has the ability to obtain information from foreign affiliates and subsidiaries, the possibility of a successful Patriot Act Request for such information cannot be ruled out. Significantly, few commentators have focused on the opposite scenario: the possibility that an EU-based cloud service provider might itself become subject to a Patriot Act request for information regarding EU citizens. In that scenario, if the EU provider maintains an affiliate, subsidiary, parent, vendor, or other connection to the U.S. (sufficient to provide a U.S. court with jurisdiction over the related entity) and that U.S.-related entity has the practical "possession, custody, or control" of the EU information, it is theoretically possible that such information could be requested, under roughly the same principles as might apply to a U.S.-based cloud service provider.

---

68 *See generally* The Sedona Conference®, "Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery," Public Comment Version (August 2008), http://www.thesedonaconference.org.

69 Sec. 442(1)(c).

70 *See* Benjamin Wallace-Wells, "Patriot Act: The Kitchen-Sink Approach To National Security," August 27, 2011, http://www.nymag.com.

71 *See, e.g.* "Analysis of Specific USA PATRIOT Act Provisions," http://epic.org (stating that the "protected computer" definition in the act "includes effectively any computer"); Sean Gallagher, "PATRIOT ACT and Privacy Laws Take a Bite Out of US Cloud Business," December 8, 2011, http://arstechnica.com.

Interestingly, at least one commentator has suggested that the concerns over the security of data stored in Europe by U.S.-based cloud service providers can be traced at least in part to early efforts at a sort of digital protectionism in the form of state efforts to promote European cloud companies over their U.S. competitors. The suggestion is that, for competitive purposes, European firms may call attention to purported insecurities of data stored with U.S.-based cloud providers flowing from the Patriot Act.[72] This suggestion was fueled by comments of German telecommunications giant, Deutsche Telekom, and other EU-based cloud providers who are marketing EU cloud services, "as a means to shield clients from government access such as that provided by the Patriot Act."[73]

COMPARISON TO LAW ENFORCEMENT REGIMES IN EUROPE AND OTHER JURISDICTIONS

Through the 1990s, European telecommunication surveillance steadily increased, as EU law enforcement recognized the importance of such information in combating drug offenses.[74] In the wake of the September 11, 2011 attacks in the U.S. (and additional major attacks in Madrid and London), many EU nations considered modifications to their law enforcement and national security laws to enhance their ability to fight terrorism.[75] These new EU laws, for example, often permit investigation of banking records related to the financing of terrorist activities and expand law enforcement ability to conduct surveillance of suspected terrorists.

Several EU nations, including Germany and the U.K., have enacted laws that permit government authorities to obtain access to personal data stored in data centers in connection with national security (and other) investigations, often without the knowledge or prior consent of the customer.[76] However, especially in Germany, data protection and the protection of privacy in general are aggressively defended. On February 27, 2008 the German *Bundesverfassungsgericht,* or German Federal Constitutional Court (similar to the U.S. Supreme Court), set high standards for the covert infiltration of IT systems by the state, namely that actual indication of a concrete danger for a legally protected interest of paramount importance exists.[77] With this decision, the *Bundesverfassungsgericht* ruled that Article 10 of the German constitution creates a right to confidentiality and integrity of IT systems, against which any intrusion by the state must be measured.[78] Still, most EU countries permit government entities access to data stored in the cloud, under certain conditions.[79] The Data Privacy Directive itself explicitly allows member states to exclude

72 *See* Kenneth Corbin, "Foreign Cloud Privacy Issues Dismissed by U.S. Officials," *CIO Magazine*, January 19, 2012, http://www.cio.com/article/698312/Foreign_Cloud_Privacy_Issues_Dismissed_by_U.S._Officials.

73 *See* Cornelius Rahn, "Deutsche Telekom Wants 'German Cloud' to Shield Data From U.S.," *Bloomberg*, September 14, 2011, http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.

74 *See* Paul M. Schwartz, "Evaluating Telecommunications Surveillance In Germany: The Lessons Of The Max Planck Institute's Study," *72 Geo. Wash. L. Rev. 1244* (2004): 1247.

75 *See generally* Kim Lane Scheppel, "Other People's PATRIOT Acts: Europe's Response To September 11," *50 Loyala L. Rev. 89* (2004) (discussing Germany and the UK, in particular); *see also* Elaine Cassel, "Patriot Act Spawns Similar Laws Across The Globe," November 10, 2003, http://www.counterpunch.org (noting that UK, Canada, Australia, South Africa, and other nations all quickly enacted "versions" of the Patriot Act, in response to terrorist attacks).

76 *See*, *e.g.*, sections 1 and 3 of the German Act on the Restriction of Privacy of Correspondence, Post and Telecommunication; U.K. Regulation of Investigatory Powers Act 2000 ("RIPA 2000").

77 BVerfG, 1 BvR 370/07 on 27.2.2008.

78 This is in line with other leading decisions of the German Supreme Court in this area, namely the "Volkszaehlungsurteil" from December 15, 1983, which created the "basic right to informational self-determination" (BvR 209, 269, 362, 420, 440, 484/83) and the March 3, 2004 ruling regarding the "Grossen Lauschangriff" which demanded the high threshold of legal justification for acoustic observation of citizens and recognizes an indefeasible core basic right to the private sphere protected by Art. 1 of the German constitution (BVerfG, 1 BvR 2378/98). The most recent decision regarding the data retention directive as implemented into German law is discussed below.

79 *See* analysis in "A Global Reality: Governmental Access to Data in the Cloud," A Hogan Lovells White Paper, Winston Maxwell, Paris France, Christopher Wolf, Washington, DC, 23 May 2012.

the application of its protective umbrella in cases of public security, defense, State security, and areas of criminal law.[80]

Sections 5 and 6 of the UK Intelligence Services Act 1994 provide for warrants authorizing surveillance acts outside the UK under certain circumstances.[81] Likewise, a recently enacted French statute permits investigating judges, with approval of the state prosecutor, to authorize police officers to use devices enabling them to access "in all places" computerized data in the form in which it appears on the screen of a user of an automated data processing system.[82] EU nations also have the power, under various mutual legal assistance agreements and treaties, to release data stored within their boundaries to U.S. authorities and vice versa, subject to conditions protecting confidentiality of personal information.[83] Thus, data stored by EU-based cloud service providers is not immune from law enforcement or intelligence surveillance by EU countries themselves.

A recent report suggests that similar law enforcement regimes apply in other countries, such as Japan and Canada.[84] Of the 10 countries studied, all 10 permit the government to require cloud providers to produce data in the course of an investigation, and 8 may do so in response to an informal request (U.S. and Japan being the exceptions).[85] Eight countries also do not require cloud providers to notify data subjects when the information is produced to government investigators, with the U.S. and Germany being the two countries that allow notification, with some exceptions.[86] Further, all 10 countries permit government investigators to monitor communications sent through the cloud, and 8 permit the government to compel cloud service providers to produce data held in other countries.[87] Additionally, the Belgian Code of Criminal Procedure provides for criminal sanctions when an electronic service provider is requested to divulge information that violates privacy rights in the course of a criminal investigation.[88]

Despite these findings, some experts still advise companies to hesitate in storing data with U.S. cloud service providers, as the U.S. is seen by many to have some of the most powerful data processing tools available and the U.S. government has generally been more aggressive than other jurisdictions in demanding data stored in other countries.[89]

Except in the case of Mutual Legal Assistance Treaties, EU countries generally confine the scope of search warrants to data within their geographic boundaries, or within

80 Article 3.2 of the EU Data Protection Directive.
81 Intelligence Services Act (UK), 1994 Chapter 13, Sections 5 and 6, available at http://www.legislation.gov.uk/ukpga/1994/13/contents.
82 *See* law no. 2011-267 (March 14, 2011), referred to as LOOPSI 2, which relates to the "orientation and planning to achieve good results with respect to internal safety." There is not yet any guidance available on the proper interpretation of "in all places," but one plausible interpretation is that the statute covers data that can be accessed by a user in France even though the data is stored outside the country. The French Code of Criminal Procedure already allowed access to documents from a data processing system.
83 *See* footnote 38, *supra*. For example, Article 10 of the E.U.-U.S. Agreement requires requested states to use best efforts to maintain the confidentiality of requests for assistance if such confidentiality is requested by the requesting state.
84 Grant Gross, "Study: Patriot Act Gives US Government No Special Access to Cloud Data," May 23, 2012, http://www.pcworld.com/.
85 *Id.*
86 *Id.*
87 *Id.*
88 Article 46bis Belgian Code of Criminal Procedure.
89 *Id.*

the possession of a party subject to jurisdiction in the country.[90] In 2007 a Belgian public prosecutor demanded U.S.-based company Yahoo!, for example, under the Belgian Code of Criminal Proceedings, provide user credentials of a number of webmail accounts. Yahoo! refused the request, arguing that the U.S. Electronic Communications Privacy Act prohibits this type of disclosure, absent a U.S. court order. After lengthy court proceedings[91] the Brussels Court of Appeals, in 2011, sided with Yahoo!, reasoning that the mere technical ability to access U.S Yahoo! servers from Belgium does not establish criminal jurisdiction in Belgian territory. [92] The Yahoo! case illustrates the need for clear definitions as to who is deemed in control of (personal) data in the often complex supply chains of providers that make up cloud services.[93]

EFFORTS AT RECONCILIATION OF CONFLICTING LAW

The Convention on Cybercrime

Shortly after the September 11, 2001 attacks in the U.S., the Council of Europe adopted the Convention on Cybercrime.[94] The convention, conceived and drafted prior to the attacks, promotes a uniform global criminal policy against cybercrime. It takes into account the rapid rate of technology changes, which blur the traditional notions of physical "care, custody, and control" of information and similar existing legal frameworks.[95] To date, more than 47 nations have become signatories to the Convention. The U.S. ratified the Convention in January 2007.

The Data Retention Directive

In 2006, the European Parliament and Council adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks (the "Data Retention Directive").[96] This Directive requires all EU member states to enact regulations to compel private service providers to store basic telecommunications metadata (dates of communications, senders and recipients, IP address), for 6-24 months after it is required for business reasons. This obligation does not apply to the content of communications. The Data Retention Directive was justified as a "valuable tool in the prevention, investigation, detection, and prosecution of criminal offences, in particular

90 Convention on Cybercrime, Art. 18 and in particular explanatory note Art. 173, which requires that a law enforcement authority can "order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory […]." It also explicitly states that "a mere technical ability to access remotely stored data (*e.g.*, the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute 'control' within the meaning of this provision;" Ian Walden, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent," Queen Mary University of London, School of Law, November 14, 2011, 5.

91 The public prosecutor opened proceedings against Yahoo! before a Belgian Criminal Court, which in 2009 ruled that Yahoo! was indeed in violation of the Belgian Code of Criminal Proceeding by failing to cooperate. This ruling was overturned in 2010 by the Court of Appeals in Ghent with the argument that the type of services Yahoo! provided did not actually fall under the definition of the Code of Criminal Proceedings in question. This in turn was toppled by the Belgian Supreme Court in 2011, arguing that the definition of the type service Yahoo! provided was in the scope of the applied criminal law, and referred back to the Brussels Court of Appeals.

92 Court of Appeal of Ghent of 30 June 2010; Ian Walden, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent," 18; this case is still ongoing.

93 *See also* Renzo Marchini, *Cloud Computing*, 49; "Industry Recommendations to Vice President neelie Kroes on the Orientation of a Eurpean Clous Computing Strategy," November 2011, 7.

94 ETS 185 (November 8, 2011), http://www.conventions.coe.int; *see also* "Law Enforcement Agencies Access Rights to Your Cloud Data," (July 22, 2011), http://blogs.computerworlduk.com/cloud-vision/2011/07/law-enforcement-agencies-access-rights-to-your-cloud-data/index.htm.

95 *Id.* at Art. 6.

96 Available at www.eur-lex.europe.eu.

organised crime."[97] In Germany, § 113a and 113b of the TKG and § 100g StPO were implemented to comply with the directive. Thereafter, almost 35,000 German citizens petitioned the German Supreme Court to repeal the Data Retention Directive as a violation of the fundamental human and constitutional right to privacy.[98]

On March 2, 2010 the German Supreme Court invalidated the Data Retention Directive,[99] ruling that it deeply invades the fundamental private sphere of a person.[100] Such an invasion can only be justified, said the German Supreme Court, under the strictest conditions which were not satisfied by the law in its current form.[101] This ruling left Germany in violation of the requirement to implement the Data Retention Directive by 2007. To date, Germany has still not complied with this requirement, giving rise to a lawsuit by the EU Commission filed on May 31, 2012, seeking sanctions of €300,000 per day. Ironically, the current Minister of Justice, Sabine Leutheusser-Schnarrenberger, was one of the plaintiffs in the appeal to the German Supreme Court which invalidated the law in Germany.

The Data Retention Directive is criticized because it requires retention of information, even if entirely irrelevant to any criminal investigation. In contrast, the Patriot Act has no comparable data retention provision and only requires retention of "specific information requested" by the U.S. government.[102] In 2011, an EU Commission investigation concluded that the Data Retention Directive is still a valuable tool, but that it needs modification "to ensure that high levels of respect for privacy and the protection of personal data are applied consistently."[103]

Work of The Sedona Conference® Working Group Six

In 2008, The Sedona Conference® Working Group Six on International Electronic Information Management, Discovery, and Disclosure (WG6) – a private, non-profit U.S.-based think-tank with international participants – issued its initial guidance on how to manage the conflict between U.S. discovery obligations and EU privacy concerns.[104] The Sedona Conference® WG6 outlined a framework for analyzing and balancing "the needs, costs, and burdens of discovery with the interests of each jurisdiction in protecting the privacy rights and welfare of its citizens,"[105] which helped spawn a constructive dialogue with EU and other international DPAs.

In early 2009, the Article 29 Data Protection Working Party Issued its Working Document 1/2009 on pre-trial discovery for cross border civil litigation[106] suggesting that compliance with the U.S./EU "Safe Harbor" program, or equivalent data protections, would be required for any transfer of EU data to the U.S. for purposes of litigation. The Working Party noted that compliance with a request under the Hague Convention would always "provide a formal basis for a transfer of personal data" but observed that not all

97 *Id.*
98 BvR 256/08, BvR 263/08, BvR 586/08.
99 BVerfG, 1 BvR 256/08.
100 BVerfG, 1 BvR 256/08, 210 ff.
101 BVerfG, 1 BvR 256/08, 269ff.
102 *See* Kristina Ringland, "The European Union's Data Retention Directive And The United States' Data Preservation Laws: Finding The Better Model," *5 Shidler J. L. Comm. & Tech. 13* (2009), http://www.lctjournal.washington.edu.
103 http://ec.europa.eu/home-affairs/policies/police/police_data_en.htm *see the full report* at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.
104 *See* The Sedona Conference®, "Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery," Public Comment Version (August 2008), http://www.thesedonaconference.org.
105 *Id.* at 29.
106 00339/09/EN, WP 158 (February 11, 2009), http://www.ec.europa.eu/justice.

member states have signed the Convention, and that many who have signed it have entered a reservation against U.S. discovery rules.

Later in 2009, a French national privacy agency (Commission Nationale de l'Informatique et des Libertés, or "CNIL") recognized that all requests for transfer of information from France to the U.S. for purposes of litigation must comply with French data protection law.[107] The CNIL suggested that such requests should be processed exclusively through the Hague Convention system, and that data protection principles, including notice to data subjects and proportionality of scope, must apply to the transfers. In 2010, both the Federal Trade Commission and the U.S. Department of Commerce offered detailed reports on the need for a more comprehensive U.S. approach to privacy protection, among other things, to deal with the problem of international exchange of information.[108] Legislative hearings, and the introduction of bills for additional privacy protection, have followed in the wake of these reports.[109] The FTC recently issued a further report.[110]

In December 2011, The Sedona Conference® WG6 issued *The Sedona Conference® International Principles on Discovery, Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation (European Union Edition)*.[111]

In early 2012, Vice-President of the European Commission Neelie Kroes, responsible for the Digital Agenda, announced her intention to make Europe not just cloud friendly, but cloud active,[112] by updating the European Data Privacy regulations.[113] Similarly, the first U.S. Chief Information Officer, Vince Kundra, announced a "Cloud-First" policy, estimating that this strategy could save the U.S. approximately $US5 billion per year.[114]

In addition to the above initiative, the U.S. and EU regulators have continued their efforts to improve coordination between in the law enforcement and counter-terrorism arena. Thus, for example, the U.S. Department of Justice and Belgian authorities recently signed The Agreement on Preventing and Combating Serious Crime, which will allow the exchange of biometric and biographic data on suspected criminals, to "bolster counterterrorism and law enforcement efforts while protecting individual privacy." The U.S. has entered into 20 such agreements with European and other nations, including Germany, the Netherlands, Finland, Spain, and Greece.[115]

These developments, reflecting a continuing need to balance law enforcement and national security against privacy protection concerns, have received the highest level of

---

107 Deliberation 2009-474 (August 19, 2009), http://www.legifrance.gouv.fr.
108 *See* Preliminary FTC Staff Report, "Protecting Consumer Privacy In An Era Of Rapid Change: A Proposed Framework for Businesses And Policymakers," December 2010, http://www.ftc.gov; Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy In The Internet Economy: A Dynamic Policy Framework," December 2010), http://www.ntia.doc.gov.
109 *See, e.g.*, McCain-Kerry Commercial Privacy "Bill of Rights" legislation, text available at http://www.kerry.senate.gov; Diane Bartz, "John McCain, John Kerry Introduce Contentious U.S. Privacy Bill," April 12, 2011, http://www.reuters.com.
110 "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
111 The Sedona Conference®, "International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation," European Union Edition, (December 2011).
112 Neelie Kroes speech in Davos, January 27, 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38; http://blogs.ec.europa.eu/neelie-kroes/european-cloud-partnership/.
113 http://ec.europa.eu/information_society/activities/cloudcomputing/index_en.htm.
114 Fran Foo, "US government's first chief information officer slams cloud computing excuses," *The Australian*, September 1, 2011.
115 *See* Department of Justice Press Release, September 20, 2011, http://www.justice.gov.

attention in the U.S. and in the EU. Recently, for example, a Dutch government minister suggested that the Dutch government should ban U.S. cloud service vendors from providing service to the government due to concerns that the Patriot Act could be used to invade the privacy of Dutch citizens.[116] Just two days later, the same official changed his position, noting that the issue "is a conflict of legislation that should initially be resolved between governments."[117]

The Data Protection Regulation

Most recently, on January 25, 2012, the EU Commission endorsed a new EU Regulation on Data Protection[118] intended to supersede the 1995 EU Data Directive.[119] Regarding the proposed EU Regulation, Peter Hustinx, EU Data Protection Supervisor, commented that : "*The proposed rules for data protection in the law enforcement area are unacceptably weak. In many instances there is no justification whatsoever for departing from the rules provided in the proposed Regulation. The law enforcement area requires some specific rules, but not a general lowering of the level of data protection*."[120]

Among the other provisions of the pending Regulation – subject to modification during the ratification process in the EU Parliament and Council of Europe – is a strong endorsement of Privacy by Design (PbD) – a concept developed originally by Dr. Ann Cavoukian, Ph.D., former Canadian Information and Privacy Commissioner.[121] This concept calls for building in, by default, data privacy and protection controls in computer systems that store, process, manage, and transfer personal data. This Privacy by Design concept was also featured in the Article 29 Working Party Document 168 as the global cornerstone for the Working Party's vision of "The Future of Privacy."[122]

Barring a significant change in the direction of cross-border initiatives, including the new EU Regulation, Cloud Computing providers will likely need to build data privacy and data protection controls into Cloud Computing platforms in order to be compliant with "Privacy by Design" as well as Patriot Act requirements.[123]

Binding Safe Processor Rules

The proposed EU Regulation introduce the concept of Binding Safe Processor Rules ("BSPRs") which instructs data processors to take necessary steps to legitimize international transfers of data by putting in place BSPRs or appropriate contractual arrangements. In the Cloud Computing context, BSPRs will essentially require Cloud Computing providers working in the EU to agree to be legally liable for any data

116 *See* Zack Whitaker, "Dutch Government To Ban U.S. Providers Over Patriot Act Concerns," September 19, 2011, http://www.zdnet.com.

117 *See* Loek Essers, "Dutch Minister Changes Patriot Act Stance," September 21, 2011, http://www.pcworld.com (noting Dutch suggestion that the European Commission should "quickly resolve the Patriot Act cloud issue").

118 *See* Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," *BNA Privacy and Security Law Report*, *11 PVLR 06*, June 2, 2012; and *see* "EU Commission Press Release" and "Press Conference Recording," available for download at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46.

119 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF; *see also* Article 29 Working Party Document 191, "Opinion 01/2012 on the Data Protection Reform Proposals," 00530/12/EN, 23 March 2012.

120 Available at http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/12/7&format=HTML&aged=0&language=EN&guiLanguage=en.

121 A biography of Cavoukian is available on the Canadian IPC website at http://www.ipc.on.ca/english/about-us/about-the-commissioner/, and more information regarding the Privacy by Design concept can be found at http://privacybydesign.ca/about/.

122 *See* Article 29 Working Party Document 168, "The Future of Privacy," 02356/09/EN, 1 December 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

123 For a discussion of the impact of the Directive on cloud service providers, *see* Thor Olaverud, "Security: Prepared for the EU's New Data Protection Regulation," www.cio.com.

breaches or losses that occur at their data centers. It effectively sets up a kind of accreditation scheme for Cloud Computing providers; to get the accreditation, vendors would have to demonstrate the adequacy of their security controls. EU experts expect that BSPRs will serve somewhat as a "bridge" for expansion of EU-based cloud providers, but that the Patriot Act broader will hinder increase reliance on U.S.-based cloud providers and services.[124]

Cloud Contracting Best Practices

Finally, as a best practice, Cloud Computing agreements must carefully be scrutinized to ensure that the provide consumers with appropriate data privacy and security protection, in accordance with applicable law. Such agreements should clearly define provisions relating to: (1) Service levels; (2) Data Security Breach Notification; (3) Legal Process Notification; (4) Use and Access to Customer Data; (5) Compliance with EU and other Applicable Data Protection Laws; (6) Limits of Liability; (7) Indemnity; (8) Representations and Warranties; (9) Termination and (1) Secure Destruction of Customer Data at Termination.[125]

CONCLUSION

Some storm clouds do appear on the horizon for cross-border discovery and data privacy, in some part due to the extraterritorial reach of the Patriot Act to U.S.-based Cloud Computing providers. Cloud service providers have the ability to store personal and personal sensitive data of citizens worldwide, anywhere in the world. As a result, cloud service providers and their customers must carefully consider the law applicable to the jurisdictions in which they do business. Cloud Computing providers, particularly those located within or with significant contacts to the U.S. should carefully consider how the U.S.A. Patriot Act, the EU Directive, and the proposed EU Regulation impact the cross-border e-discovery/data privacy landscape, and should take steps now to mitigate additional risks of conflicting legal obligations.[126]

124 Tom Brewster, "EU to legislate on Cloud Security," IT News, Sept. 30, 2011, available at: http://www.itnews.com.au/Tools/Print.aspx?CIID=275266.

125 *See* Andrew Geyer and Melinda McLellan, "Strategies for Evaluating Cloud Computing Agreements," Bloomberg Law Reports, August 5, 2011, available at: http://www.nymity.com/Free_Privacy_Resources/Previews/MaskedReferencePreview.aspx?guid=e70bb8c5-0856-4fa5-86ae-1bb87cdf237a.

126 *See: New Model Clauses for Data Processors on Their Way?,* Privacy and Information Law Blog, April 25, 2012, available at: http://privacylawblog.ffw.com/2012/new-model-clauses-for-data-processors-on-their-way.Footnotes 7/7.