Bloomberg BNA

Privacy and Security Law Report®

EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation

By Paul M. Schwartz

Cloud computing allows dramatic flexibility in information processing—and on a global basis. Its technology permits data transmissions that span the globe. Computing activities now shift from country-to-country depending on load capacity, time of day, and a variety of other factors. These decisions are sometimes made in real time and by machines rather than humans.

The cloud is also a business sector in which U.S. companies lead the world in new products and services. Important and innovative cloud offerings include Salesforce, Dropbox, Google Drive, the Amazon Elastic Compute Cloud, and Microsoft SkyDrive. The market for cloud computing is already a multibillion-dollar international market. Forrester Research Inc. has predicted a growth in the size of this market from $40.7 billion in 2011 to more than $241 billion in 2020.[1]

Due to the international dimensions of cloud computing, regulations outside of the United States are now as important as those inside it. The European Union is the most important bilateral trade area for the United States, and its proposed data protection regulation (''Proposed Regulation'') is of profound significance for U.S. companies that offer cloud services.[2] As the European Commission notes, concerns about data protection constitute ''one of the most serious barriers to cloud computing take-up.''[3] It calls for ''a chain of confidence-building steps to create trust in cloud solutions.''[4] One of the most important of these steps is the Proposed Regulation and its strong protections for information privacy.

U.S. cloud services should take particular note of two areas of the Proposed Regulation. The first concerns its limitations on the use of an individual's consent to permit data processing. The second is how it crafts a broad jurisdictional reach for EU information privacy law.

Consent

For an American cloud company, a logical step to justify information processing might be to gain permission from the user of its service. After all, ''notice-and-consent'' is an established legal principle in the United States. Under it, companies provide notice regarding their planned information use to the affected individual and then gain his or her consent for the data processing.[5]

In the European Union, the starting point is different: personal data processing is only permitted in the European Union pursuant to a legal basis. Without an authorization in an EU law or some legal provision, the use of personal information is impermissible.[6] Is consent

[1] *See* Shane O'Neill, *Forrester: Public Cloud Growth to Surge, Especially SaaS*, CIO, Apr. 26, 2011, http://www.cio.com/article/680673/Forrester_Public_Cloud_Growth_to_Surge_Especially_SaaS.

Paul M. Schwartz is professor of law at the University of California, Berkeley School of Law, and director of the Berkeley Center for Law & Technology.

[2] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (Jan. 25, 2012) [hereinafter Proposed Regulation], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (11 PVLR 178, 1/30/12).

[3] European Commission, *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe* 8 (Sept. 17, 2012) [hereinafter Unleashing the Potential of Cloud Computing in Europe], *available at* http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf (11 PVLR 1474, 10/1/12).

[4] *Id.* at 9.

[5] On the reliance in the United States on a notice-and-consent model, see Paul M. Schwartz, *The EU-U.S. Privacy Collusion*, 126 Harv. L. Rev. 1966, 1976 (2013).

[6] Proposed Regulation, *supra* note 2, at 43–44.

 ISSN 1538-3423

then a possible means for U.S. cloud companies to gain a legal basis for information processing?

The short answer is ''no.'' The Proposed Regulation sets strong restrictions on the use of the consent mechanism with the result of greatly limiting its availability for cloud companies. To be sure, the Proposed Regulation does list ''consent'' as one of the legal justifications for the processing of personal data.[7] It requires that written consent for personal information processing be presented in a form ''distinguishable'' from any other matter,[8] which is a requirement that U.S. companies should be able to meet, although it will require innovative steps on their part. Yet, its Article 7 places the ''burden of proof'' of demonstrating consent on the ''controller,'' that is, the party who determines the purposes and means of the processing of personal data.[9] This requirement makes the consent option less available and less attractive. It heightens the risk that a user's consent will not stand up if a data protection commissioner or the user herself challenges the assent after the fact. One such ground for this challenge would be that the affected party did not have an adequate basis to provided consent in a knowing and informed matter to the data processing.

Finally, and most problematically, the Proposed Regulation effectively places consent *per se* out of bounds for many, indeed perhaps most, situations involving the cloud. It states that ''[c]onsent shall not provide a legal basis for the processing'' when ''there is a significant imbalance between the position'' of the controller and the party to whom the data refers.[10] Cloud companies cannot justify processing by a party's consent if they offer take-it-or-leave-it terms for the processing of personal data, or provide cloud services for employees or other parties that lack effective bargaining power.

This skepticism toward consent is already known to EU privacy law. For example, in its investigation of Google's unified privacy policy, the French data protection commission, the CNIL, expressed strong skepticism about any reliance on consent. The critical language concerned Google Apps, which are a suite of email and office collaborations applications. Google Apps allow teams of workers to collaborate and manage information. In October 2012, the CNIL stated: ''For Google Apps end-users, the use of a Google Account is decided by the Google Apps customer (typically the company that employs the end-users): consent may therefore not be valid.''[11] The CNIL is arguing that consent from the *company* in the EU that signs up for Google Apps does not necessarily amount to valid consent from its *employee*.

In the context of public sector clouds in the European Union, consent is equally problematic. Already, the Article 29 Working Party, an EU-wide organization of national data protection commissioners, has called for ''[s]pecial precautions'' to be taken before the public sector uses cloud services.[12] These officials are also likely to reject citizen consent as a basis for permitting this processing. As in the employment context more generally, there is a significant power imbalance between federal, state, and local governments and their citizens. This imbalance would prevent reliance on the consent of the affected citizen to justify the public sector's use of cloud services. This language regarding imbalance in negotiating positions also casts doubt on any simple reliance on a contract as a legal basis for allowing the processing of personal data in the European Union. As a consequence, U.S. cloud companies cannot rely on one-sided click-through agreements.

It is therefore back to square one: the processing of personal information in the European Union means compliance with measures in EU law that permit such activity. In particular, as Article 6(3) of the Proposed Regulation states, the law that justifies the processing must be ''in the public interest, . . . respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.''[13] This language means that cloud companies are obliged to meet the strict ''fair information practices'' of EU information privacy law.

As a silver lining, the Proposed Regulation recognizes the important existing instruments that harmonize EU and U.S. privacy law. These are the the U.S.-EU Safe Harbor Program, binding corporate rules, and model contracts.[14] While their use entails higher requirements and burdens for companies than consent, these mechanisms are all available under the Proposed Regulation. Moreover, the European Commission has called for development of ''safe and fair contract terms and conditions'' for use of cloud services.[15] The European Data Protection Supervisor has also emphasized the need for improvement and standardization of the contract terms of cloud service providers.[16] In contrast, reliance merely on the consent of the affected party would be made on thin ice.

Jurisdiction

The Proposed Regulation creates a jurisdictional net that sweeps broadly.[17] It applies to ''processing activities'' that are related to ''the offering of goods or services'' to individuals within the European Union or ''the monitoring of their behavior.''[18] The result potentially subjects all cloud services to EU privacy law.

The difficulties here are numerous. The Proposed Regulation does not provide any further definitions or explanations of the term, ''offering of goods or ser-

[7] *Id.* art. 6(1)(a), at 44.
[8] *Id.* art. 7(2), at 45.
[9] *Id.* art. 7, at 45.
[10] *Id.* art. 7(4), at 45.
[11] Commission nationale de l'informatique et des libertés (CNIL), *Google Privacy Policy: Main Findings and Recommendations* 8 (Oct. 16, 2012), *available at* http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf (11 PVLR 1559, 10/22/12).
[12] Article 29 Data Prot. Working Party, *Opinion 05/2012 on Cloud Computing* 23 (July 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (11 PVLR 1097, 7/9/12).
[13] Proposed Regulation, *supra* note 2, art. 6(3), at 44.
[14] *See id.* art. 42(2), at 70–71.
[15] Unleashing the Potential of Cloud Computing in Europe, *supra* note 3, at 11.
[16] *See* Article 29 Data Prot. Working Party, *supra* note 12, at 23 (emphasizing the need for standardization of contract terms regarding law enforcement access to personal data).
[17] For more detailed analysis of the jurisdictional provisions of the Proposed Regulation, see Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1613 (2013).
[18] Proposed Regulation, *supra* note 2, art. 3(2), at 41.

  PVLR ISSN 1538-3423

vices.'' Since the cloud is available anywhere in the EU that an internet connection can be found, any cloud company is presumably ''offering'' its product within the European Union and covered by the Proposed Regulation.

Finally, the Regulation equates its concept of ''monitoring'' of behavior broadly with ''profiling.'' The EU definition of this concept reaches tracking on the internet ''with data processing techniques . . . , particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.''[19] Many kinds of value-added services that draw on the user's information may be ''profiling,'' and, hence, ''monitoring'' in this sense of the Proposed Regulation.

In short, the current formulation of the Proposed Regulation extends EU information privacy law to a wide range of circumstances in which networked intelligence on the internet shapes applications and services for EU users. In many instances, however, there may not be a privacy impact on an EU citizen: a cloud service may only be providing computing power for an EU company. Nonetheless, these companies may still face complex obligations under EU privacy law. The European Union's arcane distinctions between ''controllers'' and ''processors'' add a further degree of regulatory complexity in this area.[20]

Three adjustments are necessary to EU privacy law. As part of their ongoing consideration of the Proposed Regulation, the European Council, Parliament, and Commission should adopt these proposals.

First, the Proposed Regulation should borrow an existing jurisdictional exemption from the EU Data Protection Directive (95/46/EC). Current EU law withholds jurisdiction if ''equipment is used only for purposes of transit through the territory of the Community.''[21] Certain cloud services fit neatly within this exemption. An example would be companies that provide Infrastructure as a Service (IaaS). In IaaS, a cloud provider might offer server and network components, virtualization, file systems, and capacity on demand. The EU Electronic Commerce Directive (2000/31/EC) also frees an intermediary service provider if it is a ''mere conduit'' that transmits information.[22]

Second, the Proposed Regulation's concept of the ''offering'' of services should be replaced with the ''directing'' of services. An earlier ''Interservice Draft'' of the Proposed Regulation contained the latter term.[23] Relevant existing tests in other areas of EU law as to its meaning include acceptance of the euro for services, or facilitating access within the European Union for the service or product, such as through use of a top-level domain name of an EU member state.[24] The benefit of the idea of ''directing'' services is that it focuses on whether a non-EU organization has chosen to enter the EU market.

Finally, the European Union should modify its view that ''monitoring'' is synonymous with ''profiling.'' It should view ''monitoring'' more narrowly and restrict it to situations where observations of an individual are linked to privacy risks. For example, mere observation without decisionmaking about a person should be excluded from the definition of ''monitoring.'' Such observational steps might include initial stages of collection and analysis of information where there is no privacy risk for an identified person. An example would be the collection of information to reject unsafe browsers from logging on to cloud services.

Conclusion

The Proposed Regulation will alter the landscape in the European Union for U.S. cloud services. First, the Proposed Regulation drastically narrows the conditions for reliance on the use of ''consent'' mechanisms as a justification for data processing. It does permit, however, recourse to existing harmonization instruments such as the U.S.-EU Safe Harbor Program, binding corporate rules, or model contracts. Second, the Proposed Regulation extends EU privacy jurisdiction quite broadly. Should these provisions not be reformed before adoption of the final regulation, EU privacy law will widely apply to non-EU cloud companies. While it is necessary and appropriate for the European Union to protect the online privacy interests of its citizens, the European Union should not become the super-regulator of all cloud companies regardless of the extent of an impact on its citizens.

---

[19] *Id.*, recital 21, at 20.

[20] *See* Council Directive 95/46, art. 2(d)–(e), 1995 O.J. (L 281) 31, 38 (EC).

[21] *Id.* art. 4(1)(c), at 39.

[22] Council Directive 2000/31, art. 12(1), 2000 O.J. (L 178) 1, 12 (EC). The Electronic Commerce Directive sets up a test with three prongs for deciding when an entity is such a ''mere conduit.'' These requirements are that it ''(a) does not initiate a transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.'' *Id.*

[23] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, art. 2(2), at 36 (Nov. 29, 2011) (''directed''), *available at* http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf. For background on this concept, see *id.* recitals 14–15, at 20.

[24] *See, e.g.*, Joined Cases C-585/08 & C-144/09, Pammer v. Reederei Karl Schlüter GmbH & Co. KG, 2010 E.C.R. I-12520, I-12584, para. 29, I-12589, para. 47 (determining whether the operation of a website could be considered activity ''directed to'' a member state). The opinion is available online in the original German at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:DE:PDF, as well as in English, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:EN:HTML.