ARTICLE

# INFORMATION PRIVACY IN THE CLOUD

PAUL M. SCHWARTZ†



† Professor, University of California, Berkeley, School of Law; Director, Berkeley Center for Law & Technology. Many thanks to Marty Abrams, Paula Bruening, Helen Nissenbaum, Paul Ohm, Richard V. Purcell, Joel Reidenberg, and Daniel Solove for their helpful suggestions.

## INTRODUCTION

Cloud computing is the locating of computing resources on the Internet in a fashion that makes them highly dynamic and scalable. This kind of distributed computing environment can quickly expand to handle a greater system load or take on new tasks. Cloud computing thereby permits dramatic flexibility in processing decisions—on a global basis. The rise of the cloud has also significantly challenged established legal paradigms. This Article analyzes current shortcomings of information privacy law in the context of the cloud. It also develops normative proposals to allow the cloud to become a central part of the evolving Internet. These proposals rest on strong and effective protections for information privacy that are also sensitive to technological changes.

This Article takes a comparative focus: it examines legal developments in the United States and the European Union. As the White House noted in its 2012 consumer privacy framework, the United States "is a world leader" in cloud computing.[1] While leading cloud companies are U.S.-based, the European Union sets strong requirements for flows of personal data, and these obligations have already had a major impact on U.S. companies. The European Union's significant role in international decisions around information privacy has been bolstered by the authority of EU member states to block data transfers from their country to third-party nations.[2] Such nations include the United States, which the European Union generally considers to lack "adequate" privacy protections.[3] Moreover, the European Commission's release in late January 2012 of its "General Data Protection Regulation"[4] provides a perfect juncture to assess the issue of privacy in the cloud.

---

1 WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 6 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

2 *See* Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 45-46 (EC) (instructing member states to permit the transfer of data to a third party country only if the Commission finds that that country provides adequate protection).

3 *See* Working Party on the Prot. of Individuals with Regard to the Processing of Data, Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" Issued by the US Department of Commerce on 19th April 1999, at 2, (EC) No. 5047/99, WP 19 (May 3, 1999), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp19en.pdf ("reiterat[ing] its view that the patchwork of narrowly focused sectoral laws and self-regulatory rules presently existent in the United States cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union").

4 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed Data Protection*

This Article examines three areas of change in personal data processing due to the cloud. In doing so, it draws on an empirical study in which I analyzed the data processing of six major international companies.[5] The first area of change concerns the nature of information processing at companies. For many organizations, data transmissions are no longer point-to-point transactions within one country; they are now increasingly international in nature. As a result of this development, the legal distinction between national and international data processing is less meaningful than in the past. Computing activities now shift from country to country depending on load capacity, time of day, and a variety of other concerns. The jurisdictional concepts of EU law do not fit well with these changes in the scale and nature of international data processing.

A second legal issue concerns the multidirectional nature of modern data flows, which occur today as a networked series of processes made to deliver a business result. Due to this development, established concepts of privacy law, such as the definition of "personal information" and the meaning of "automated processing" have become problematic. There is also no international harmonization of these concepts. As a result, EU and U.S. officials may differ on whether certain activities in the cloud implicate privacy law.

A final change relates to the shift toward a process-oriented management approach. Users no longer need to own technology, whether software or hardware, that is placed in the cloud. Rather, different parties in the cloud can contribute inputs and outputs and execute other kinds of actions. In short, technology has provided new answers to a question that Ronald Coase first posed in *The Nature of the Firm*.[6] In that classic essay, Coase sought to shed light on a fundamental question of corporate organization—when a firm will produce something for itself, and when it will procure from another. New technologies and accompanying business models now allow firms to approach "make or buy" decisions in innovative ways. Different functions and operations can be packaged as modular units that can be

*Regulation*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

5 *See* PAUL M. SCHWARTZ, THE PRIVACY PROJECTS, MANAGING GLOBAL DATA PRIVACY: CROSS-BORDER INFORMATION FLOWS IN A NETWORKED ENVIRONMENT 13-15 (2009), *available at* http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf. I conducted the study on behalf of The Privacy Projects, an independent nonprofit organization centered on enhancement of privacy through research and education. *Id.* at 3, 71. In this Article, I have also drawn on research regarding developments in cloud computing subsequent to this study.

6 *See generally* R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937), *reprinted in* THE NATURE OF THE FIRM: ORIGINS, EVOLUTION, AND DEVELOPMENT 18 (Oliver E. Williamson & Sidney G. Winter eds., 1993).

pulled apart and reassembled. Yet information privacy law tends to assess legal responsibility in a static fashion. In particular, privacy law's approach to liability for privacy violations and data losses in the new "make or buy" world of the cloud may not create adequate incentives for the multiple parties who handle personal data.[7]

Thus, this Article's focus is a comparative one from which it explores significant changes in data processing due to the cloud and the resulting tension with contemporary information privacy law. This Article concentrates on issues relating to the private ordering of data processing. There are, therefore, important restrictions on its scope. It discusses neither national security nor criminal law issues. To be sure, the cloud changes the ability of intelligence agencies and law enforcement officials to access personal data, but these matters are conceptually different enough from those involving purely private parties as to merit separate analysis. This Article also does not analyze issues that arise when the government uses cloud services. Here, too, there are distinct policy and legal issues.

## I. THE USE OF THE CLOUD

The term "cloud" comes from the traditional representation of the Internet in network diagrams. Network diagrams typically depict in detail the servers, client PC's, and routers that are internal to an organization, and then illustrate the Internet simply with a cloud.[8] Over time, people realized that they could move computer resources that had been inside an organization to the Internet—that is, onto the "cloud." The National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction."[9]

The cloud has already had an impact on many people. By 2008, the Pew Internet & American Life Project had found that "[s]ome 69% of online Americans use webmail services, store data online, or use software programs such as word processing applications [the] functionality [of which] is located

---

7 On the "make or buy" decision and how Coase views it as turning on the relative cost of the use of the market versus the cost of using the firm's managerial organization, see Harold Demsetz, *Coase, Ronald Harry*, *in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 267 (Peter Newman ed., 1998).

8 ANTHONY T. VELTE ET AL., CLOUD COMPUTING: A PRACTICAL APPROACH 3-4 & fig.1-1 (2010).

9 PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

on the web."[10] The trend has continued: more people expect that, in the future, they will access software applications online and share information through remote server networks rather than on their personal computers.[11]

The cloud has also been an incredible economic success story. The research firm Forrester forecasts that the global market for cloud computing "will leap from $40.7 billion [in 2011] to more than $241 billion in 2020."[12] In Germany, the largest economy in the European Union, investments in and the services of the 2010 cloud market were worth €1.14 billion.[13] This market is estimated to be worth €3 billion by the end of 2012 and €8 billion by 2015.[14] Beyond these statistics, however, a 2012 *New Yorker* cartoon represents perhaps the ultimate sign of the cloud's arrival as a social phenomenon. In it, a child says to her teacher, "The Cloud ate my homework."[15]

In this Part, I analyze how the cloud changes the processing of personal data by organizations. Three alterations in particular point to the need for adjustments to information privacy law. The first concerns the increased international scale of information processing. The second concerns the development of personal information processing as a networked event. Continuous, multipoint data flows are now commonplace, and decisions about information processing, such as those concerning the collection of data or its transfer, are made in a decentralized fashion through networked intelligence. Finally, there has been a change in management processes to allow outsourcing of computing resources. Today, the cloud permits operations to be packaged as modular units that can be pulled apart and reassembled in different ways. Contemporary technology permits flexibility in data processing that was previously unknown. Taken collectively, these changes suggest the need for modifications to information privacy law.

---

10 Data Memo from John B. Horrigan, Assoc. Dir., Pew Internet & Am. Life Project, Regarding Use of Cloud Computing Applications and Services 1 (Sept. 2008), http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.

11 *See* JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING 8 (2010), http://www.pewinternet.org/~/media/Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf (reporting survey results finding that a majority of respondents expect most people to be working predominantly on the cloud by 2020).

12 *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.

13 Press Release, Experton Group, Cloud Computing Startet in Deutschland Durch—Ausgaben und Investitionen in 2010 Bereits über Eine Milliarde Euro 1 [Cloud Computing Starts Again in Germany—Spending and Investments in 2010 Already over One Billion Euros] (Oct. 6, 2010), http://www.experton-group.de/fileadmin/experton/press/2010/pm-2010-10-06-Cloud.pdf.

14 *Id.* at 2 fig.

15 Tom Cheney, Cartoon, THE NEW YORKER, Oct. 8, 2012, at 54.

### A. *International Processing of Personal Data*

In the past, companies generally worked with discrete, localized data sets and processes. An international data flow was an occasional event—an exception rather than the rule—and data processing systems were generally nationally based. From today's perspective, moreover, these past transfers were relatively static events—they did not occur continuously and they involved a fairly limited number of participants in the processing.

The Fiat incident from the late 1980s is a good illustration of this past model. At that time, Fiat-France sought to transmit human resources information about its employees to its parent company, which was located in Turin, Italy.[16] While Italy had not yet enacted a national data protection statute, France had such a law in place. The French data protection authority, the National Commission on Informatics and Liberties (*Commission nationale de l'informatique et des libertés*) (CNIL), intervened and issued a formal declaration that required Fiat-France and Fiat-Italy to sign a contract before the transfer could occur.[17] In this contract, the entities were obliged to "respect the provisions protecting human rights and fundamental liberties" required by the Council of Europe's privacy convention and French data protection law.[18] Once the two Fiat entities had signed the appropriate contract and presented it to the CNIL, the French data protection agency gave its formal approval and issued a "receipt" that allowed the transfer.[19] The transfer was a limited event—it might as well have involved a one-time shipment of physical tapes via an international courier.

In the age of the cloud, it would be anachronistic to imagine that a governmental body could issue a formal declaration and a physical receipt before each international transfer of information. The frequency, complexity, and volume of global data transfers have grown massively.[20] In particular,

---

16 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 10E RAPPORT D'ACTIVITÉ [NATIONAL COMMISSION ON INFORMATICS AND LIBERTIES, 10TH ACTIVITY REPORT] 32 (1989). Reports of the National Commission are available online back through 1999, *see Rapports d'activité*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, http://www.cnil.fr/en-savoir-plus/rapports-dactivite/accessible/non (last visited Apr. 10, 2013), but older reports (including the 1989 report) may be obtained by contacting the site's administrators at http://www.cnil.fr/pied-de-page/contactez-nous/contact-webmestre.

17 *Id.*

18 *Id.* at 32-34 (original: "respecter les dispositions protectrices des droits de l'homme et des libertés fondamentales").

19 *Id.* at 32 ("récépissé"). For a discussion, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 491-92 (1995).

20 For an overview of the relatively limited transborder exchanges in the 1980s, see REINHARD ELLGER, DER DATENSCHUTZ IM GRENZÜBERSCHREITENDEN DATENVERKEHR: EINE RECHTSVERGLEICHENDE UND KOLLISIONSRECHTLICHE UNTERSUCHUNG [DATA

we have moved from an age of international transfers of personal data to one of international processing of personal data. In many instances, the processing itself takes place within the cloud.

This distributed computing environment permits great flexibility in processing decisions—and it does so on a global basis. For example, computing activities can be shifted from country to country depending on load capacity, time of day, and any number of other concerns. An influential committee of EU data protection authorities, the Article 29 Working Party, has explained this dynamic process: "[C]loud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm."[21] Computing resources are now accessible globally, and the processing of personal information increasingly occurs through such distributed resources.

To better understand this shift in global data access and processing, we may consider an empirical study that I conducted on emerging corporate data practices across national borders.[22] All the companies that participated in this study did so anonymously and are identifiable solely by an assigned Greek letter. This study's Alpha Corporation, a pharmaceutical company, provides an excellent demonstration of continuous, international data flows. Alpha had a Global Clinical Data Management team that "implemented over 350 Electronic Data Capture . . . systems for clinical trials."[23] In 2008, these clinical trials created more than five million data points, or more than seventy-two data points every minute.[24] Alpha placed dedicated computing resources in a private cloud created by data servers located around the world; the resulting network infrastructure was for the exclusive use of this single organization with multiple business units. Alpha Corporation's data transfers followed its system requirements concerning technology, operations, resources, and administration.[25] In the absence of the cloud, this kind of intensive international data processing would simply not have been possible.

---

PRIVACY IN CROSS-BORDER DATA TRAFFIC: A COMPARATIVE AND CONFLICTS OF LAW ANALYSIS] § 3, at 108-29 (1990).

21 Article 29 Data Prot. Working Party, Opinion 05/2012 on Cloud Computing 17, (EC) No. 01037/12, WP 196 (July 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

22 *See* SCHWARTZ, *supra* note 5; *see also supra* note 5.

23 SCHWARTZ, *supra* note 5, at 13.

24 *Id.*

25 As Alpha Corporation stated, "Canadian systems might back up to a European-based server, even though the systems are geographically much closer to a United States server." *Id.* at 20.

### B. *Networked Data Processes*

In the past model, a processing decision occurred at a discrete moment and involved a unidirectional transfer of data. Companies would also finalize data processing plans in advance. Today, networked series of data processes allow the decentralization of decisions about information processing.

The Fiat incident, discussed above, provides a good illustration of this kind of static process characteristic of practices in the past. Fiat leadership planned a transfer involving a database of human resource information exclusively through a single channel from France to Italy.[26] Today, however, as the Article 29 Working Party notes, "The cloud client is . . . rarely in a position to be able to know in real time where the data are located or stored or transferred."[27] In many instances, networked intelligence itself shifts data processing and makes decisions based on its own algorithms' assessments of results from past data processing.

Consider Beta Corporation, an international marketing services company from my study of global data flows.[28] In one of Beta's typical telemarketing campaigns, planned for Spain, a marketer in Beta's Spanish office began by selecting customers to target from a list stored on servers in the United States, based on criteria developed by a vendor in India.[29] The marketer then transferred the resulting list over the Internet to a call system in Mexico for execution of the telemarketing campaign in Spain.[30] As results from the telemarketing effort in Spain trickled back to the call center in Mexico, the data was fed back into the global Customer Relationship Management system, which then helped to guide the path of the ongoing marketing campaign by providing frequent and even daily batch updates.[31] Beta, like Alpha, relied on the international transmission of personal data to reach a desired business result. Moreover, the Beta case study also shows processing decisions being made not in advance, but based on feedback from networked intelligence.

Epsilon Corporation offers another useful example. At its customer call centers, Epsilon's computers analyzed call loads and other relevant factors to determine how to distribute customer inquiries throughout the world.[32] Beyond evaluating load information, the system also drew on networked

---

26 *See supra* text accompanying notes 16-19.

27 Article 29 Data Prot. Working Party, *supra* note 21, at 17.

28 SCHWARTZ, *supra* note 5, at 13.

29 *Id.*

30 *Id.*

31 *Id.*

32 *See id.* at 14.

information about holidays and working hours in different nations.[33] This latter corporate approach to global workflow, the "follow-the-sun" model, passes tasks off between sites in different time zones based on where workdays are in progress.[34]

Networked intelligence can also be used to improve organizational decisionmaking: Through analytics, organizations seek to convert their information into actionable knowledge.[35] The cloud can promote the use of analytics in a number of ways, including through an organization's use of a "common knowledge management application" that allows global access to corporate knowledge.[36] It also enables access to "outsourced and offshore analytical resources."[37]

Among nonconsumer uses of this technology, analytics play an important role in healthcare research, the management of physician performance and clinical metrics, data security, and fraud prevention. The use of analytics in healthcare research alone has already created great social benefits. There has been a shift away from traditional clinical trials that follow specific patients toward informational research that analyzes large data and biological sample sets. The Institute of Medicine explains these new "information based" forms of inquiry as "the analysis of data and biological samples that were initially collected for diagnostic, treatment, or billing purposes, or that were collected as part of other research projects."[38]

This technique, centered on analytics, is widely used today in categories of research including epidemiology, healthcare services, and public health services. These information-based forms of health research "have led to significant discoveries, the development of new therapies, and a remarkable improvement in health care and public health."[39] As use of electronic health

---

33 *Id.* at 22-23.

34 *Id.*

35 *See* THOMAS H. DAVENPORT & JEANNE G. HARRIS, COMPETING ON ANALYTICS 7 (2007) (describing analytics as "the extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions"). For a discussion of the rise of analytics, see Paul M. Schwartz, *Privacy, Ethics, and Analytics*, IEEE SECURITY & PRIVACY, May/June 2011, at 66, 66-69.

36 DAVENPORT & HARRIS, *supra* note 35, at 161.

37 *Id.* at 180.

38 INST. OF MED. OF THE NAT'L ACADS., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 112 (Sharyl J. Nass et al. eds., 2009).

39 *Id.* at 113. For example, through analysis of the records of a cohort of 9000 breast cancer patients, scientists were able to identify the HER-2 oncogene. Scientists then developed a targeted therapy, Herceptin, that is effective for women with HER-2 breast cancer. *Id.* at 114. In another major research effort, started in 2003, "the National Institutes of Health, the Food and Drug Administration, the drug and medical-imaging industries, universities and nonprofit groups joined in . . . a collaborative effort to find the biological markers that show the progression of

information increases, the ability to carry out analytics on medical data will grow. As one physician stated regarding the willingness in the field of informatics to take "lots of data" instead of "perfectly controlled data": "You can deal with the noise if the signal is strong enough."[40] For example, one recent retrospective study on over 900,000 patients drew on data from multiple healthcare systems with different electronic health records.[41] The authors of the paper were able to identify an association between certain patient characteristics, especially height and body mass index, and "venous thromboembolic events."[42] The authors concluded that this kind of information-based research "has the potential to allow population research with minimal resources—time, people and money."[43]

### C. *Modular Units and Outsourced Services*

The third major technological change is that users no longer need to own technology, whether software or hardware, if it is placed in the cloud. In one analogy, computer services are now available from the network in the same way that electricity is available from an outlet.[44] The examples of Alpha, Beta, and Epsilon Corporations demonstrate some of the ways in which companies draw on cloud services. These organizations used networked servers to store applications and data and permit global access to these resources by authorized users using multiple devices, whether Macs, PCs, phones, or tablets. Alpha, Beta, and Epsilon Corporations developed

---

Alzheimer's disease in the human brain." Gina Kolata, *Rare Sharing of Data Led to Results on Alzheimer's*, N.Y. TIMES, Aug. 13, 2010, at A1. The key element of the project was the commitment of participants to share all the data from it with the public. *The New York Times* observed, "The key to the Alzheimer's project was an agreement as ambitious as its goal: . . . to share all the data, making every single finding public immediately, available to anyone with a computer anywhere in the world." *Id.*

40 Peter Jaret, *Mining Electronic Records for Revealing Health Data*, N.Y. TIMES, Jan. 15, 2013, at D1.

41 *See* David C. Kaelber et al., *Patient Characteristics Associated with Venous Thromboembolic Events: A Cohort Study Using Pooled Electronic Health Record Data*, 19 J. AM. MED. INFORMATICS ASS'N 965 (2012).

42 *Id.* at 967-72.

43 *Id.* at 972; *see* Bradley A. Malin et al., *Biomedical Data Privacy: Problems, Perspectives, and Recent Advances*, 20 J. AM. MED. INFORMATICS ASS'N 2, 5 (2013) ("[N]ew computing infrastructures and high-throughput technologies are creating new challenges to privacy that the biomedical community will need to handle in the not too distant future.").

44 *See, e.g.*, ARBEITSKREISE TECHNIK UND MEDIEN DER KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER, ORIENTIERUNGSHILFE—CLOUD COMPUTING [WORKING GRPS. OF THE TECH. AND MEDIA CONF. OF DATA PROT. COMMR'S OF THE FED. & STATE GOV'TS, GUIDANCE—CLOUD COMPUTING] 4 (ver. 1.0, Sept. 26, 2011); Rama Ramaswami & Dian Schaffhauser, *What Is the Cloud?*, CAMPUSTECHNOLOGY (Oct. 31, 2011), http://campustechnology.com/articles/2011/10/31/what-is-the-cloud.aspx.

"private" clouds: the networked resources that they placed on the Internet were reserved for internal use and located behind a corporate firewall.[45]

Over the last five years, however, the billion-dollar development has been the growth in public clouds. A host of new enterprises have made these technologies widely available to businesses and consumers alike. Leading services include Apple iCloud, Dropbox, Google Drive, Microsoft Skydrive, and Salesforce. Research and development continues; for instance, Intel has recently introduced a hardware-software cloud solution based on integration at the processor level.[46]

Public clouds are based on three different service models. In the accepted nomenclature, these are known as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[47] In SaaS, the end user, often a consumer, uses the provider's applications that run within the cloud. Clients access these applications through a client interface, such as a Web browser. Web-based email is an example of SaaS through a client interface. Another example is Google Drive. In the business world, customer relationship management applications are the most important use of SaaS;[48] Salesforce is a leading vendor in this area.[49]

In PaaS, the provider delivers a development and deployment stack, in which the consumer receives integrated software for development and use. The consumer has control over the deployed applications.[50] Examples of PaaS include the Google App Engine and Force.com, which is the development environment for Salesforce.[51] Finally, in IaaS, the consumer can deploy and run software including operating systems and applications. The customer of IaaS rents and uses external computing resources instead of purchasing them and having her own employees maintain them within her own organization.[52] Perhaps the most successful IaaS operation at present is

---

45 SCHWARTZ, *supra* note 5, at 29-30, 33-34.

46 INTEL, SECURITY IN THE CLOUD: INTEL XEON PROCESSOR E5-4600/2600/2400/1600 (2012), *available at* http://www.intel.com/content/dam/doc/solution-brief/cloud-computing-security-in-the-cloud-brief.pdf.

47 For these standard definitions, see VELTE ET AL., *supra* note 8, at 11-16.

48 *See Salesforce Product Overview*, SALESFORCE, http://www.salesforce.com/products (last visited Apr. 10, 2013).

49 On the rise of Salesforce, see the account of its founder, MARC R. BENIOFF & CARLYE ADLER, BEHIND THE CLOUD: THE UNTOLD STORY OF HOW SALESFORCE.COM WENT FROM IDEA TO BILLION-DOLLAR COMPANY—AND REVOLUTIONIZED AN INDUSTRY (2009).

50 *See generally* LEE BADGER ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. NO. 800-146, CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS §§ 6.2–.3 (2012), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075.

51 *See* VELTE ET AL., *supra* note 8, at 72-74.

52 *See id.* at 214-16. This service can also permit "dynamic scaling" to permit immediate access to more resources as well as a "pay-as-you-go" approach to pricing. *Id.* at 220. Technically, such

Amazon's Elastic Compute Cloud. Although Amazon is best known as a leading online retailer of consumer goods, it also sells "resizable compute capacity in the cloud."[53]

Recall the analogy regarding how the cloud supplies computing like electricity from an outlet. A company or person does not need to buy machines or software and then manage computer resources to process personal data. Rather than requiring coordination of these services and goods within the client firm itself, the cloud permits the client to purchase computing resources on a "spot market."[54] Companies therefore have new flexibility in deciding on the shape and form of computing work. As a result, different functions and operations concerning the processing of personal information can be packaged as modular units that can be pulled apart and reassembled.

## II. THE MISMATCH WITH INFORMATION PRIVACY LAW

In this Part, I analyze three areas in which there is a regulatory mismatch between cloud services and information privacy law. The first concerns jurisdiction: Which privacy law should apply to personal information in the cloud? Here, the regulations in the European Union prove especially complex and confusing. The second area of regulatory tension concerns a threshold matter around key definitional terms: When should privacy law apply? Third, the cloud provides new flexibility for companies seeking to determine whether to manage computing activities inside or outside their corporate structure: Will law provide incentives to create adequate safeguards for personal data?

### A. *Jurisdiction: Which Nation's Privacy Law Applies?*

In the EU model, a nation's data protection law is expressed in omnibus privacy statutes.[55] These laws establish regulatory standards for privacy with

immediate response to greater demand poses a range of interesting challenges for computer scientists. Luis M. Vaquero et al., *Dynamically Scaling Applications in the Cloud*, COMPUTER COMM. REV., Jan. 2011, at 45, 48-49.

53 *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2 (last visited Apr. 10, 2013).

54 Demsetz characterizes "firm-like coordination" as consisting of "[s]pecialization, continuity of association, and reliance on direction" as opposed to "self-sufficiency and spot markets" for activities outside of the enterprise. Harold Demsetz, *The Theory of the Firm Revisited*, *in* THE NATURE OF THE FIRM, *supra* note 6, at 159, 171.

55 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1110 (4th ed. 2011).

a broad scope; typically, a single omnibus law in an EU member state will regulate personal data use in the public and private sectors alike.[56] Within the European Union, sectoral laws serve as backup to regulate specific areas of data use and to increase the specificity of regulatory norms within that state.[57] Sectoral laws might regulate, for example, how telecommunications companies use personal information.

Unlike the European Union, the United States lacks an omnibus information privacy statute and instead regulates this area through sectoral laws alone.[58] States and the federal government have different statutes for the public and private sectors. Within the private sector, regulations concentrate on the data holder and, in some instances, on the type of data. Within the private sector, for example, there are information privacy laws and regulations for educational records, video rental records, and healthcare records.[59]

Notwithstanding its scattered provisions today, U.S. law played an important international role in the initial development of information privacy law. The U.S. Department of Health, Education, and Welfare's concept of "fair information practices" (FIPs), first articulated in 1973,[60] has influenced the development of a common set of high level principles for information privacy law.[61] FIPs "are the building blocks of modern information privacy law," albeit expressed somewhat differently in each statute.[62]

The clear international preference today is to follow the EU approach. Worldwide, most countries outside the EU have enacted omnibus statutes, many of which resemble the EU approach to information privacy law.[63] Moreover, the international preference has been for the specific variations of FIPs identified by the European Union.

---

56 *Id.*

57 *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908-16 (2009).

58 *See id.* at 904-05; *supra* note 3.

59 *See, e.g.*, 20 U.S.C. § 1232g (2006) (providing for family educational and privacy rights); 18 U.S.C. § 2710 (creating a civil action to redress the "[w]rongful disclosure of video tape rental or sale records"); Privacy of Individually Identifiable Health Information, 45 C.F.R. pt. 164, subpt. E (2012).

60 *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 50 (1973) (proposing a regulation to define "fair information practice").

61 On the historical role of the Department of Health, Education & Welfare's report, see DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306 (1989).

62 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999). The precise content of the resulting obligations will often differ based on the context of data processing, the nature of the information collected, and the specific legislative, regulatory, and organizational environment in which the rules are formulated.

63 *See* Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 72-79 (2012) (charting the influence of the EU Directive of 1995 on data protection laws across the world).

As a further matter, and in contrast to the EU approach, the United States emphasizes a "notice-and-choice" model for its FIPs. As the Federal Trade Commission describes this approach, it "encourages companies to develop privacy notices describing their information collection and data use practices to consumers, so that consumers can make informed decisions."[64] In the European Union, prominent FIPs require that personal data be processed only pursuant to a legal basis, that there be an independent data protection authority in each nation to oversee data use, that there be limits on automated decisionmaking, and that sensitive data receive additional protection.[65] Such FIPs are not present in the United States—at least not as formal legal requirements.[66] Thus, the United States' unique path as a matter of form (no omnibus law) and substance (a limited set of FIPs) has made it an outlier in relation to the global community.[67]

In the United States, moreover, the cloud's dramatic increase in international data transfers has not led to significant regulatory difficulties, or new complexities, for information privacy law. First, U.S. information privacy law does not give government officials the power to block international transfers of personal information.[68] In the context of the outsourcing of U.S. information processing to India and other countries, Congress occasionally evinces concern about this lack of legal restrictions, but it has yet to enact a law regulating international transfers of personal data.[69] In

---

64 FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, at iii (2010). For a description and critique of this model, see *id.* at 19-21 ("[C]onsumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered to them."); and Schwartz, *supra* note 62, at 1621-35 ("[M]ost people are unable to control, and are often in ignorance of, the complex processes by which their personal data are created, combined, and sold.").

65 For a description of the EU model of FIPs, see CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW ch. 2 (2d ed. 2007).

66 While there is no such formal legal requirement, an increasing number of leading U.S. companies have sophisticated privacy management programs, including a Chief Privacy Officer. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261-63 (2011). These processes are not the formal equivalent, however, of EU-style FIPs.

67 *See* Greenleaf, *supra* note 63, at 70-72 ("Increasingly, . . . the USA is the only significant outrider attempting to defend providing data privacy protection by a patchwork of sectoral laws (with significant limits to their principles arising from circumstances which may be unique to the USA) and no national [data protection authority] as a key means of enforcement.").

68 *See* Schwartz, *supra* note 57, at 910-11.

69 Such a proposal was included, however, in an early draft of the bill that later became the Privacy Act of 1974. *See* S. 3418, 93d Cong. § 201(a)(6) (1974), *reprinted in* S. COMM. ON GOV'T OPS. & HOUSE COMM. ON GOV'T OPS., SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RIGHTS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 14 (Comm. Print 1976). On outsourcing to India and privacy concerns, see SOLOVE & SCHWARTZ, *supra* note 55, at 1161-63.

contrast, the 1995 EU Data Protection Directive requires each member state to give its data protection authority such power.[70] The 2012 Proposed Regulation on Data Protection permits an international transfer of data from the European Union only if the Commission has made a finding of adequacy, use is made of "appropriate safeguards," or one of its enumerated exceptions applies to the transfer.[71]

Second, U.S. law does not generally require that a law regulate information processing before it takes place. No omnibus statute in the United States contains such a mandate. Personal information processing is freely permitted unless a law specifically forbids the activity or otherwise sets parameters on it.[72] At the same time, however, there is an increasingly dense patchwork of laws and regulations in the United States. State information privacy law is now of increasing importance due to the high level of regulatory activity and the possibilities that companies will simply choose to organize their information practices to conform to the strictest privacy standard in the most important jurisdiction for their business.[73]

To illustrate current state privacy laws, we can begin with those state data security laws that impose a substantive requirement of "reasonable security" before any data processing may occur. In California, for example, any "business that owns or licenses personal information about a California resident" is required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[74] Numerous other state laws contain specific requirements to ensure the safe disposal of personal data.[75]

---

70 *See* Council Directive 95/46, *supra* note 2, art. 25, at 45-46.

71 *Proposed Data Protection Regulation*, *supra* note 4, arts. 41-44, at 69-74. The Proposed Regulation now permits an adequacy determination for less than an entire country, but merely "territory," "processing sector," or "international organization in question." *Id.* art. 41(1), at 69.

72 Schwartz, *supra* note 57, at 908-16 (contrasting an EU approach to information privacy based on the prevention of harm with a U.S. approach of "regulatory parsimony," and, in particular, avoiding unnecessary regulation of information flows).

73 Federal environmental law even sometimes grants one state a special regulatory power; this phenomenon permits one state to serve as a "superregulator." Ann E. Carlson, *Iterative Federalism and Climate Change*, 103 NW. U. L. REV. 1097, 1107-14 (2009) (explaining California's role as a "superregulator" for mobile source emissions).

74 CAL. CIV. CODE § 1798.81.5(b) (West 2009).

75 *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 72.004 (West 2009); WASH. REV. CODE ANN. § 19.215.020 (West 2007); *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 182-83 (2d ed. 2013) (reviewing state data disposal statutes). On the differing EU and U.S. approaches to data protection, and for an argument that EU officials are operating at a higher speed in modernizing their laws, see Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES, Mar. 31, 2013, at BU1.

As this California law indicates, moreover, state data security laws and state data breach notification laws in the United States do apply to non-U.S. data processors. The question of who is protected by that California statute is as straightforward as with similar state laws: Is the personal data of a resident of the respective state involved? The data disposal law cited in the preceding paragraph, for example, applies to any business that processes information about a California resident. California's highly influential breach notification statute also follows this approach.[76] It requires that "following discovery or notification of the breach in the security of the data," the business notify "any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[77] The application of such a law to the cloud remains straightforward: it depends on whether a data breach involves the personal data of a resident of California. The location of the entity that processes the information is irrelevant.

In the European Union, the question of the application of privacy law to the cloud is more complex. Indeed, numerous commentators have noted the difficulties of this aspect of EU data protection law. For example, in his treatise on EU data protection law, Christopher Kuner writes, "The legal rules for determining whether EU law applies to business activities, if so which national law, and where jurisdiction lies, are extraordinarily complex, and involve a number of difficult questions to which there are no definite answers."[78] In a similar vein, Antonis Patrikios has noted that the 1995 EU Data Protection Directive's rules are "particularly problematic in modern business arrangements of a distributed and truly international nature, such as . . . cloud computing."[79]

For the regulation of the cloud, the two fundamental EU legal documents are the 1995 Data Protection Directive[80] and the Proposed Data Protection Regulation of 2012.[81] The Directive, which establishes common rules for information privacy among EU member states,[82] is the most important privacy regulation in Europe; it has largely replaced the Council

---

76 *See* CAL. CIV. CODE § 1798.29(a).

77 *Id.*

78 KUNER, *supra* note 65, § 3.01.

79 Antonis Patrikios, *Application of the Law*, *in* EUROPEAN PRIVACY: LAW AND PRACTICE FOR DATA PROTECTION PROFESSIONALS 65, 67 (Eduardo Ustaran ed., 2012).

80 *See supra* note 2.

81 *See supra* note 4.

82 *See* Council Directive 95/46, *supra* note 2, art. 32(1), at 49 ("Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive . . . .").

of Europe's Convention on Data Protection of 1980 as the central document of European information privacy law. The future of EU privacy law rests not with the Directive, however, but with the Proposed Data Protection Regulation.

A popular tool of EU lawmaking, directives are generally "harmonizing" instruments rather than directly binding commands; they require member states to enact national legislation that reflects their principles.[83] After enactment of the Data Protection Directive in 1995, all EU member states enacted conforming legislation.[84] In January 2012, the Commission of the European Union released a Proposed Data Protection Regulation, which will be directly binding on member states.[85] Since the process of enactment of the Regulation will take a number of years, and its final form is unknown, this Article analyzes the applicable jurisdictional law of the cloud under both the Directive and Proposed Regulation.

### 1. The Data Protection Directive (1995)

The Data Protection Directive stakes out a number of bold positions, including establishing a limit on international data transfers to countries that lack "adequate" legal protections for personal information.[86] The key provision for this jurisdictional question is the Directive's Article 4(1)(c).[87] Article 4(1)(c) determines when companies with headquarters outside of the European Union fall under EU data protection law. It applies EU privacy law to a "controller" who "is not established on Community territory," but who "for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State."[88] Yet Article 4(1)(c) raises more questions than it provides answers.

---

83 Schwartz, *supra* note 19, at 481-82; *see, e.g.*, *supra* note 82.

84 For an official list of all the national legislation enacted by EU member states to conform with the 1995 Data Protection Directive, see *National Execution Measures*, EUR-LEX, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:71995L0046:EN:NOT (last visited Apr. 10, 2013). Regarding the drawn-out process of the enactment and amendment of national data protection law to conform with the Directive, and the remaining differences between the national laws, see Spiros Simitis, *Einleitung: Geschichte—Ziele—Prinzipien*, *in* NOMOS KOMMENTAR: BUNDESDATENSCHUTZGESETZ [NOMOS COMMENTARY: FEDERAL DATA PROTECTION ACT] 169-70 (Spiros Simitis ed., 7th ed. 2011). Thus, even after harmonization, differences can remain in the laws of member states. For the purposes of this Article, however, it will be enough to concentrate on the Directive's approach.

85 *See* Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, 11 PRIVACY & SECURITY L. REP. 215, 216 (2012).

86 *See supra* text accompanying note 2.

87 Council Directive 95/46, *supra* note 2, art. 4(1)(c), at 39.

88 *Id.*

Indeed, as Kuner remarks, "No provision" of the entire Directive "has caused more controversy than Article 4(1)(c)."[89]

a. *Who Is a Controller?*

In the terminology of EU information privacy law, a "controller" is a "natural or legal person . . . or any other body" that "determines the purposes and means of the processing of personal data."[90] More specifically, EU law defines the controller as the entity who decides how personal data is collected, stored, used, altered, or disclosed.[91] Controllers have far more legal obligations and responsibilities than processors. As the Article 29 Working Party summarizes, "[T]he first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice."[92] The European Union draws a contrast in this regard with the "processor" who merely processes data on behalf of the controller.[93]

A difficulty for cloud computing is the uncertainty in EU law as to when a cloud provider is a controller or a processor. A team of researchers at Queen Mary College of Law, University of London, has carried out an in-depth study of this issue.[94] As they note, a cloud processor can be a controller, a processor, or in some instances, both. Under EU privacy law, a cloud provider is only the processor if there is a separate entity, a user, who determines the "purposes of the processing" or its essential "means."[95] Under the 1995 Directive, for example, a cloud service is a data controller if it provides an online calendar where it synchronizes appointments and contacts across multiple devices.[96] Yet "purposes" and "means" of processing are difficult conceptual categories to apply to cloud computing, where responsibilities are distributed and then shared and shifted—sometimes in real time. At a minimum, the legal analysis here must be highly context specific.[97]

---

89 KUNER, *supra* note 65, § 3.23.

90 Council Directive 95/46, *supra* note 2, art. 2(d), at 38.

91 *See id.* art. 2(b), at 38 (defining "processing of personal data").

92 Article 29 Data Prot. Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor," WP 169, (Feb. 16, 2010), at 4 (emphasis omitted), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

93 Council Directive 95/46, *supra* note 2, art. 2(e), at 38.

94 *See* W. Kuan Hon et al., *Who Is Responsible for 'Personal Data' in Cloud Computing?—The Cloud of Unknowing, Part 2*, 2 INT'L DATA PRIVACY L. 3 (2012).

95 Council Directive 95/46, *supra* note 2, art. 2(d)–(e), at 38.

96 Patrikios, *supra* note 79, at 73.

97 In this regard, the Article 29 Working Party is less than helpful in its analysis, which simply finds that "there may be situations in which a provider of cloud services may be considered either

b. *When Is There a "Use of Equipment Situated Within the Territory" of the European Union?*

Just as uncertainty exists as to the terms "controller" and "processor," there is little clarity about other concepts found in the Directive's Article 4(1)(c). For example, the Article's language regarding "use of equipment" shows a pre-Internet understanding of information processing. Kuner observes, "What evidently was *not* contemplated at the time of drafting was the existence of a ubiquitous, seamless information network (i.e., the internet) which, owing to its decentralized nature, would routinely allow EU citizens to transfer data back and forth to millions of computers throughout the world."[98] The cloud has further complicated the analysis regarding the "use of equipment." Today, when a user in the European Union draws on the cloud, she can access networked resources, and the network can draw on the user's own PC, smartphone, or tablet. In 2005, Joel Reidenberg had already noted that "more sophisticated computing enlists the processing capabilities and power of users' computers."[99] Today, the cloud permits the user's own equipment to become part of a processing operation.

The issue becomes even more complex when the "equipment" in question may include software that the cloud provider supplies. Consider the case of cookies, which are alphanumerical text files installed on a user's hard drive. The Article 29 Working Party has declared that EU information privacy law should regulate cookies as "equipment" that triggers the applicability of EU legal protections.[100] In a summary of the relevant law, an international privacy lawyer has noted how broadly "equipment" can be defined: "[I]n principle, almost any hardware, software or system could qualify as 'equipment situated' on the territory of a member state."[101] A 2009 amendment to the E-Privacy Directive of 2002 brought cookies under EU privacy law. It defines the regulated activity as the "storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user."[102]

---

as a joint controller or as a controller in their own right depending on concrete circumstances." Article 29 Data Prot. Working Party, *supra* note 21, at 8. For some advice from an international privacy lawyer on how a service provider can remain in the role of a data processor and keep its customer in the role of the controller, see Lothar Determann, *Data Privacy in the Cloud—Myths and Facts*, PRIVACY L. & BUS. INT'L REP., Feb. 2013, at 17, 20 (Myth 10).

98 KUNER, *supra* note 65, § 3.26.

99 Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1953 (2005).

100 Article 29 Data Prot. Working Party, Working Document, Privacy on the Internet—An Integrated EU Approach to On-line Data Protection 28, WP 37 (Nov. 21, 2000), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf.

101 Patrikios, *supra* note 79, at 74.

102 Council Directive 2009/136, art. 2, 2009 O.J. (L 337) 11, 30 (EC).

### 2. The Proposed General Data Protection Regulation (2012)

On January 25, 2012, the Commission of the European Union released its Proposed General Data Protection Regulation. This document marks an important policy shift from a directive to a regulation. In EU law, a directive requires harmonizing legislation, but a regulation establishes directly enforceable standards.[103] Thus, upon enactment, the Data Protection Regulation will be binding national law within each Member State and will take precedence over any contrary elements of national information privacy law.[104]

The Commission wished to shift to a regulation for data protection because the Directive had not caused sufficient harmonization throughout the European Union. Due to the Directive's failure to create uniformity, a regulation was needed to create legal certainty within the internal market and to assure a continuing role for the European Union "in promoting high data protection standards worldwide."[105] In particular, the Directive's granting the member states "room for manoeuvre in certain areas" and the power to issue "particular rules for specific situations" had created "additional cost and administrative burden" for private stakeholders.[106] Moreover, for the Commission of the European Union, the need for more uniform regulations was acute because "rapid technological developments and globalisation have profoundly changed the world . . . and brought new challenges for the protection of personal data."[107] Among the new problem areas, the Commission pointed to cloud computing, which "may involve the loss of individuals' control over their potentially sensitive information when they store their data with programs hosted on someone else's hardware."[108]

There were also specific harmonization problems relating to the cloud. Acknowledging the kinds of difficulties under the Directive that this Article's preceding section identified, the Commission noted:

> The Internet makes it much easier for data controllers established outside the European Economic Area (EEA) to provide services from a distance and to process personal data in the online environment; and it is often difficult

---

103 *See, e.g.*, Kuner, *supra* note 85, at 215, 217; Katerina Linos, *How Can International Organizations Shape National Welfare States?*, 40 COMP. POL. STUD. 547, 562 (2007).

104 Kuner, *supra* note 85, at 216.

105 *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 5, COM (2010) 609 final (Oct. 4, 2010).

106 *Id.* at 10.

107 *Id.* at 2 (emphasis omitted).

108 *Id.*

> to determine the location of personal data and of equipment used at any given time (e.g. in 'cloud computing' applications and services).[109]

In short, the Commission acknowledged the need for a new approach to privacy in the cloud. The merits of its current proposal are another matter.

The Proposed Regulation will greatly expand the jurisdiction of the European Union's data protection law over non-EU companies that provide services through the cloud. Rather than the "use of equipment" benchmark of the Directive, the Proposed Regulation's Article 3(2) has two alternate tests for whether EU data protection law is to apply to data controllers not established in the Union. When the personal data of EU "data subjects" are processed, the Proposed Regulation applies if "the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour."[110] These new tests, "the offering of goods or services" and "monitoring," will sweep more non-EU companies offering services through the Internet into the jurisdiction of EU data protection law.[111] At the same time, the Proposed Regulation raises new questions regarding the future regulation of the cloud.

a. *What Is an "Offering of Goods or Services"?*

The Proposed Regulation does not provide any further definitions or explanations of this term. Its language is potentially quite broad, however, because the cloud is available anywhere in the European Union that an Internet connection can be found. "Offering" is also broader in applicability than the potential test of "activities which are directed to" EU residents,

---

109 *Id.* at 11 (footnote omitted).

110 *Proposed Data Protection Regulation*, *supra* note 4, art. 3(2), at 41. An amendment to the Proposed Data Protection Regulation from the EU Parliament would further broaden both requirements. It makes clear that jurisdiction applies even if the "offering of goods and services" is free of charge. It further alters the wording of the language regarding monitoring of behavior to "the monitoring of such data subjects." This proposed amendment is intended to extend the regulation to not only "the monitoring of the behaviour of Union residents by data controllers outside of the Union, such as through internet tracking, but all collection and processing of personal data about Union residents." *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011—C7-0025/2012—2012/0011(COD))*, No. PR\922387EN.doc, amend. 83, at 63/215 (Jan Philipp Albrecht rptr., Dec. 17, 2012), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf; *see also id.* amend. 82, at 63/215.

111 *See* Kuner, *supra* note 85, at 219 (noting that the wording of Article 3(2) has resulted in "uncertainty").

which was the approach found in the leaked "interservice" version of the Regulation from late 2011.[112]

b. *What Is "Monitoring" of Behavior?*

Recital 21 of the Proposed Regulation equates "monitoring" with profiling.[113] The consequences of this test for the cloud are potentially far-reaching. Any "value added" service that draws on the user's information is arguably "monitoring" in this sense. For example, a cloud service that tracks an individual's data use to provide additional storage capacity has "profiled" that person. As a result, EU privacy law will apply to a wide range of circumstances in which networked intelligence on the Internet shapes applications and services.

### B. *Networked Intelligence in the Cloud: When Does Privacy Law Apply?*

A further problem raised by the cloud is how it challenges basic definitions of information privacy law. At a fundamental level, information privacy law concerns the processing of personal data. Yet, the cloud raises questions as to the meaning of both "personal data" and the "processing" of that data.

The basic threshold for the application of privacy law in the European Union concerns whether "personal data" are present. Personal data is defined in EU law as information that refers to "identified or identifiable" persons.[114] More explicitly, it states that "an identifiable person is one who can be identified, 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."[115] As long as the information refers to identified or identifiable persons, information privacy

---

112 *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. 57(2)(a), at 78, version 56 (Nov. 29, 2011) [hereinafter *Interservice Draft*], *available at* http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

113 The Regulation's test is "whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes." *Proposed Data Protection Regulation*, *supra* note 4, recital 21, at 20.

114 Council Directive 95/46, *supra* note 2, art. 2(a), at 38. EU data protection law treats "identified" and "identifiable" as equivalent. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1874 (2011).

115 *Id.*

law is applicable. The Directive and Proposed Regulation alike share this approach.

The Proposed Regulation takes the same tack, but provides additional detail. In this regard, it follows its general path of greater specificity, wherever possible, compared with the Directive. Under the Proposed Regulation, the definition of persons "identified" or "who can be identified" turns on the critical concept of direct or indirect identification by "means reasonably likely to be used."[116] German law strongly influenced EU law in this area; it has long looked to "means reasonably likely to be used" in defining whether or not information is identifiable.[117] The Proposed Regulation also sets out some additional categories relevant to the required analysis: it specifies that identification may be "by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."[118] This additional specificity provides useful categories for the required assessment of when information refers to a specific person.

In the United States, the key is whether information relates to an *identified* person. There is a variety of tests in federal and state statutes and regulations for deciding when information relates to an identified person. The law does not require identifiability, and as a general matter, the U.S. threshold approach to defining personal information is reductionist when compared with the European Union's expansionist approach.[119] In the United States, the law typically finds personal information to be at stake only when the information refers to a currently identified person.[120]

There are also similarities in both the EU and U.S. legal approaches to determining the moment when information falls within the scope of information privacy law. Rather than relying on a fixed line between personal information and nonpersonal information, both systems establish a delineation that depends on a number of factors, including technology and corporate practices.[121] Whether information becomes personal information in a networked environment depends on decisions made throughout the world, sometimes in real time. It is thus increasingly difficult to decide prior

---

116 *Proposed Data Protection Regulation*, *supra* note 4, art. 4(1), at 41.

117 Ulrich Dammann, *Weitere Begriffsbestimmungen*, *in* NOMOS KOMMENTAR: BUNDESDATENSCHUTZGESETZ, *supra* note 84, § 3, marginal no. 22.

118 *Proposed Data Protection Regulation*, *supra* note 4, art. 4(1), at 41.

119 *See* Schwartz & Solove, *supra* note 114, at 1872-77 (contrasting the U.S. approach of only covering "information that refers to a currently identified person" with the EU extension beyond identified persons to all identifiable persons).

120 *Id.* at 1873.

121 *Id.* at 1845-47.

to certain kinds of cloud data processing whether or not personal data will be implicated. Thus, the cloud threatens to destabilize the regulatory approaches to personal information in the European Union and United States alike.

From the perspective of EU law, the cloud has increasingly become a "means reasonably likely to be used" and can be considered to make more information "identifiable." Yet *identifiable* information is not yet *identified* information—and indeed, some instances in the former category (identifiable) may never fall into the latter (identified). Further, varying risks are associated with the possible identification of data as opposed to information already related to an identified person.[122]

At the same time, the U.S. approach appears too limited. Some information may only be identifiable and not identified, but also bring with it a substantial risk of identification. For example, on the Internet, at some point, a person's online browsing can be tied to her name. For an illustration, consider *The Wall Street Journal*'s 2012 report on Dataium, an aggregator of online shopping behavior.[123] This company tracks individuals on the web by placing cookies on their computers. Once a person provides a name or email to a retailer, such as a car dealer, Dataium is able to tie its analysis of her web surfing to her identity and display it in the dealer's database.[124] At some point in its process of observation, Dataium obtains personally identifiable information of the type that belongs in the identified category.

To address these policy issues, Daniel Solove and I have developed an approach to personal information that we term "PII 2.0," for "Personally Identifiable Information 2.0." We argue that a category of data that should be treated as legally equivalent to identified information is "identifiable information with a substantial risk of being identified."[125] At present, however, U.S. law does not acknowledge this classification.

Beyond the cloud's destabilization of existing legal categories of "personal information" in the European Union and United States alike, there is a problematic EU restriction concerning "automated processing."[126] The European Union regulates and limits a wide range of information processing based on this category, which dates from the early years of data protection law. This French innovation, beginning with Law 78-17 of January 6, 1978,

---

122 *See id.* at 1841-45 (explaining how individuals can be re-identified by putting together various pieces of de-identified information).

123 Jennifer Valentino-Devries & Jeremy Singer-Vine, *They Know What You're Shopping For*, WALL ST. J., Dec. 8-9, 2012, at C1.

124 *Id.*

125 Schwartz & Solove, *supra* note 114, at 1886.

126 Council Directive 95/46, *supra* note 2, art. 15, at 43.

on Information Technology, Data Files, and Civil Liberties,[127] has been a part of that country's data protection law ever since. Restrictions on automated processing are also found in both the Directive and Proposed Regulation. As the Proposed Regulation's Article 20 states:

> Every natural person shall have the right not to be subject to a measure . . . which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[128]

Due to this language, use of networked intelligence located in the cloud will frequently be "automated processing" subject to heightened EU data protection safeguards. In this fashion, the Proposed Regulation creates a potential threat to socially productive uses of analytics—and ones that do not raise significant risks of individual privacy harms.

### C. *"Make or Buy": Who Is Liable?*

Recall the example of the Fiat-France data transfer to Fiat-Italy in 1989. In that case, the data flow was between branches of the same company in different countries, and the personal information went from one established database into another.[129] A touchstone marking the change from that kind of data flow to today's world is then–IBM CEO Samuel Palmisano's 2006 essay, *The Globally Integrated Enterprise*, in *Foreign Affairs*.[130]

Palmisano began by setting the revolution in information technology (IT) that began in the 1970s within the broader context of that era's liberalization of trade and investment flows. In his view, the IT revolution "standardized technologies and business operations all over the world, interlinking and facilitating work both within and among companies."[131] The resulting combination of shared technologies and common business standards, which were "all built on top of a global IT and communications infrastructure, changed the sorts of globalization that companies found possible."[132]

---

127 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227.

128 *Proposed Data Protection Regulation*, *supra* note 4, art. 20(1), at 54.

129 *See supra* notes 16-19 and accompanying text.

130 Samuel J. Palmisano, *The Globally Integrated Enterprise*, FOREIGN AFF., May/June 2006, at 127, 129.

131 *Id.*

132 *Id.*

International data flows reflect these new possibilities. As Palmisano generally notes, firms were "actively managing different operations, expertise, and capabilities so as to open the enterprise up in multiple ways."[133] Not surprisingly, Palmisano made certain that IBM drew on his insights. In 2005, it sold off certain operations, including its line of ThinkPad laptops,[134] and reinvented itself as a "global technology and innovation company."[135] As IBM's LinkedIn company profile now explains, "Utilizing its business consulting, technology and R&D expertise, IBM helps clients become 'smarter' as the planet becomes more digitally interconnected."[136] IBM's shift to a software and services model also proved to be the path to continuing financial success for the company.[137]

At a deeper level, the transformation of IBM reflects how technology provides new answers to the classic Coasean question of "make or buy." In his 1937 essay, *The Nature of the Firm*, Coase sought to shed light on the fundamental question of when a firm will produce something for itself and when it will procure from another. In a conclusion as valid today as when this essay first appeared, Coase stated that the answer to the "make or buy" question turned on the extent of a company's ability to economize on a variety of transaction costs.[138] New technologies and accompanying business models now allow firms to approach "make or buy" in innovative ways. In particular, cloud technology permits previously unknown flexibility for organizations. As the *Wall Street Journal* put it in a headline, "To Cloud, or Not to Cloud."[139] This new flexibility allows firms to decide how, when, and to what extent to structure relationships within their walls, and how, when, and to what extent to draw on outside parties and the market. In particular, data flows can be disaggregated and decoupled to allow companies to develop novel business approaches to operations and activities.

Interestingly enough, Coase thought that technology, or at least the technology of his day, would generally cause firms to bring more activities

---

133 *Id.* at 131.

134 *See* John G. Spooner & Michael Kanellos, *IBM Sells PC Group to Lenovo*, CNET (Dec. 8, 2004), http://news.cnet.com/ibm-sells-pc-group-to-lenovo/2100-1042_3-5482284.html (quoting Palmisano's description of the sale as an opportunity in the "rapidly changing information technology industry"); Steven Musil, *Lenovo Completes Buy of IBM's PC Business*, CNET (May 1, 2005), http://news.cnet.com/2100-1042_3-5691487.html.

135 IBM, *IBM*, LINKEDIN, http://www.linkedin.com/company/ibm (last visited Apr. 10, 2013).

136 *Id.*

137 Bridget van Kralingen, *IBM's Transformation—From Survival to Success*, FORBES.COM (July 7, 2010), http://www.forbes.com/2010/07/07/ibm-transformation-lessons-leadership-managing-change.html.

138 Coase, *supra* note 6, at 390-97.

139 Robert Plant, *To Cloud, or Not to Cloud*, WALL ST. J., Apr. 25, 2011, at R9.

within their walls. This distinction is critical with regard to the role of the cloud. In 1937, Coase wrote, "Changes like the telephone and the telegraph which tend to reduce the cost of organising spatially will tend to increase the size of the firm. All changes which improve managerial technique will tend to increase the size of the firm."[140] Coase saw technology, first, as bringing within a single firm many transactions previously carried out for it externally by a number of other organizations and, second, as bringing transactions previously carried out by the market within a single firm.

The cloud points to a different resolution of the question of technology's impact. The larger trend today is to permit organizations to keep computing functions *outside their walls*—that is, to "buy" and not to "make." A wide range of data processing operations can now be kept outside the walls of the organization and purchased within the "spot market," as Coase would put it, such that the Coasean firm can focus on its own expertise. Today, the Coasean firm can let Salesforce program and run its customer relations management software from the cloud while the firm concentrates on selling its products or services. It can take this path by saving its capital resources by buying computing power from Amazon or Google data centers instead of building its own. As for cloud companies, they now have their own version of "make or buy." These entities are buying chips from Intel and other hardware directly from Asian manufacturers. In so doing, they can bypass traditional computer and server manufacturers.[141]

This resulting world of "buy" has significant implications for information privacy law. It means that Coasean organizations will increasingly hire outside companies to assist in managing personal data. For the Article 29 Working Party, this trend means "a lack of control over personal data."[142] It stated, "[C]loud clients may no longer be in exclusive control of [personal] data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data."[143] In short, the Working Party's concern is that the "make or buy" world of the cloud may not create incentives for the multiple parties who handle personal data to provide adequate privacy and security.

---

140 Coase, *supra* note 6, at 397.

141 *See* Cade Metz, *Intel Confirms Decline of Server Giants HP, Dell, and IBM*, WIRED (Sept. 12, 2012), http://www.wired.com/wiredenterprise/2012/09/29853.

142 Article 29 Data Prot. Working Party, *supra* note 21, at 2.

143 *Id.* at 5 (footnote omitted).

## III. SOLUTIONS FOR INFORMATION PRIVACY LAW

In this Part, I propose solutions for the mismatch between the cloud and existing regulatory paradigms in the European Union and the United States. The critical problems relate to jurisdiction, core definitional concepts in information privacy law, and the proper role of contracts.

### A. *Jurisdiction*

As discussed above, EU regulations potentially subject all cloud services used by an EU resident to the EU's data protection law. In particular, under the Proposed Regulation, the new jurisdictional trigger would be the "offering of goods or data services" or the "monitoring of behaviour."[144] As we have seen, these proposed standards create notable regulatory ambiguities.

Here, the European Court of Justice provided a helpful perspective in its 2003 decision regarding questions referred by Sweden from its prosecution of Mrs. Bodil Lindqvist.[145] The opinion interpreted certain elements of the 1995 Data Protection Directive, in particular Article 25,[146] in light of alleged privacy violations caused by Mrs. Lindqvist's webpage. Her Internet site contained information to help members of her church prepare for their confirmation as well as information about her and her colleagues in the parish,[147] including descriptions "in a mildly humorous manner" of her colleagues' jobs, hobbies, family circumstances, telephone numbers, and other matters, including the statement that a "colleague had injured her foot."[148]

The European Court of Justice decided not to apply Article 25's restrictions on data transfers to Mrs. Lindqvist's conduct. But it did not reach this conclusion by parsing terms like "use of equipment" or the other concepts examined above.[149] Rather, the Court of Justice decided that application of Article 25 would lead to an absurdity. First, it explained,

> If Article 25 of Directive 95/46 were interpreted to mean that there is a "transfer [of data] to a third country" every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to

144 *See supra* note 110.

145 Case C-101/01, *In re* Lindqvist, 2003 E.C.R. I-12992, *available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=EN.

146 *See supra* note 2.

147 *Lindqvist*, 2003 E.C.R. at I-13002, para. 12.

148 *Id.* at I-13002, para. 13.

149 *See supra* Section II.A.

> all the third countries where there are the technical means needed to access the internet.[150]

The Court of Justice then pointed to the resulting incongruous outcome: "[If] even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet."[151]

A similar absurdity follows if placing personal data into the cloud broadly subjects all non-EU cloud providers to EU regulation. The difficulty is that the Proposed Regulation's concepts of "offering" and "monitoring" are general enough to permit this interpretation. At the same time, it is appropriate for states to protect the online privacy interests of their citizens. We should remember Reidenberg's warning against "Internet separatists" who would seek legal immunity, or something close to it, for all online activity.[152]

Three adjustments are necessary to permit protection of privacy by EU member states while also avoiding creation of a jurisdictional net that is too wide. The first is to replace "offering" with "directing," a term from the earlier "Interservice Draft" Data Protection Regulation.[153] The second is to narrow the definition of "monitored." The final is to reintroduce the concept of "transit" of data into the Proposed Regulation.

As noted above, an earlier draft of the Data Protection Regulation reached only entities located outside of the European Union that were directing activities to within the European Union and not merely offering products or services.[154] The benefit of this test is that it focuses on whether a non-EU organization chose to enter the EU market, either by accepting the Euro as payment for services or transacting business in a different language than the one it normally uses. Another factor that would point to directing of a cloud service is a step to facilitate access within the European Union to the service or product, such as the use of a top-level domain name of an EU member state. Additional relevant factors for defining "directing activities" can be developed through reference to EU case law regarding directing activities to EU residents.[155]

---

150 *Id.* at I-13020, para. 69 (alteration in original).

151 *Id.*

152 *See generally* Reidenberg, *supra* note 99, at 1953.

153 *See Interservice Draft*, *supra* note 112, art. 2(2), at 36. For background on this concept, see *id.*, recitals 14-15, at 20.

154 *See supra* text accompanying note 112.

155 *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=

The second step should be rethinking the concept of "monitoring." The danger is that the European Union, in interpreting this term as synonymous with "profiling," will view any use of networked intelligence to tailor services as triggering its regulation. "Monitoring" should be read in a narrower fashion. Networked intelligence leads to the collection of observations; some of these observations create privacy threats for EU data subjects and some do not. Ultimately, EU law should restrict its grant of jurisdiction to situations where these observations are linked to privacy risks.

To this end, the European Union should begin by excluding from the definition of monitoring certain initial steps of data processors that occur before they make decisions about a specific person. These steps might include the collection, integration, and analysis of information.[156] For example, servers can be programmed to reject unsafe browsers.[157] This choice should not, however, be considered "monitoring." Though it constitutes observation, it does not create a privacy risk for a specific individual, or in the language of information privacy law, for an "identified" person.

Finally, the EU Data Protection Directive exempts from its grant of jurisdiction situations where data are only in transit. This exception is grafted onto the Directive's rules for jurisdiction over a "controller" who uses equipment situated in the European Union. Jurisdiction is not present when "such equipment is used only for purposes of transit through the territory of the Community."[158] Yet the Proposed Regulation drops this concept entirely from its definition of its territorial scope. In some cloud services, however, the provider is handling data that is in transit. An example would be IaaS, where the provider offers server and network components, virtualization, file systems, and capacity on demand.[159] While the provider of these services should meet data security requirements, such as are found in EU telecommunications law, the jurisdiction of EU privacy law should not generally apply to this organization.[160]

---

CELEX:62008CJ0585:DE:PDF, as well as in English, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:EN: HTML.

156 For a discussion of these concepts in the context of analytics, see Paul M. Schwartz, *Data Protection Law and the Ethical Use of Analytics*, 10 PRIVACY & SECURITY L. REP. 70 (2011).

157 *See, e.g.*, MICHAEL BARRETT & DAN LEVY, PAYPAL, A PRACTICAL APPROACH TO MANAGING PHISHING § 4.1 (2008), *available at* https://www.paypal-media.com/assets/pdf/fact_sheet/a_practical_approach_to_managing_phishing_april_2008.pdf (suggesting that servers should reject "unsafe browsers" that do not block phishing sites).

158 Council Directive 95/46, *supra* note 2, art. 4(1)(c), at 39.

159 *See supra* notes 47-53 and accompanying text.

160 Researchers at Queen Mary Law School have taken a different approach to reach a similar result. They argue that under certain circumstances, such as when a cloud provider merely hosts data, the provider should not be considered to be either a "controller" or a "processor." An example

A comparison with the eCommerce Directive of 2000 is also useful.[161] The eCommerce Directive frees an intermediary service provider from liability if it meets three conditions. The Directive states that an entity that is a "mere conduit" and simply transmits information should not be held liable so long as 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."[162] Like the idea of exempting a non-EU controller of equipment from jurisdiction where the equipment transmits information through the territory of the European Union, the "mere conduit" test frees from jurisdiction an entity that merely offers computing from an outlet.

### B. *Networked Data Processes and PII 2.0*

There is a mismatch between the cloud and the respective statutory definitions of "personal information" in the European Union and the United States. There is also a problem concerning the definition of "automated processing" in the European Union. Regarding personal information, lawmakers in the European Union and the United States should think about identification in terms of risk level. Here, the Schwartz-Solove model, Personally Identifiable Information (PII) 2.0, presents a new and useful approach to defining key threshold terms.

In our view, privacy law should not extend indiscriminately to "identifiable" information, as it does in the European Union, and should not be limited only to information that currently identifies a person, as it is in the United States. Personal information should be defined as relating to identified persons, that is, information that "singles out a specific individual from others."[163] Put differently, a person has been identified when her identity has been ascertained. At the same time, there should be some protections even for "identifiable information."[164] The key to understanding this distinction turns on Fair Information Practices (FIPs), which we have already discussed in the context of EU-U.S. information privacy law.

The basic toolkit of FIPs in the United States includes (1) limits on information use; (2) data minimization (i.e., limits on data collection); (3) limits on disclosure of personal information; (4) data quality principles (i.e.,

would be a company, such as Amazon, offering IaaS. They "believe an exemption or exception to data protection laws is justified" for the mere hosting of data. Hon et al., *supra* note 94, at 11.

161 *See* Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC) [hereinafter "eCommerce Directive"].

162 *Id.* art. 12(1), at 12.

163 Schwartz & Solove, *supra* note 114, at 1877.

164 *Id.* at 1886.

collection and use only of information that is accurate, relevant, and up-to-date); (5) notice, access, and correction rights for the individual; (6) transparent processing systems (i.e., the creation of processing systems that the concerned individual can know about and understand); (7) security for personal data; and (8) enforcement mechanisms.[165] When information refers to an *identified* person, all of the FIPs generally should apply.

As for *identifiable* data, PII 2.0 would only apply to those FIPs "that concern data security, transparency, and data quality."[166] Data quality, the FIP that deserves the most explanation, requires organizations to engage in good practices of information handling. This requirement should be commensurate with the purpose of the information processing: the higher the risks for the affected individual, the higher the data quality should be. The model of PII 2.0 also includes an important distinction regarding certain instances in which identifiable information should be treated like information referring to an identified person. If there is a substantial risk that certain information will lead to identification of an individual, it should be treated as referring to an identified person.[167] From the start, this information should be shifted from the identifiable to the identified category because of the significant probability that a party will link it to a person.

Once the concept of PII 2.0 is applied to the cloud, the law will distinguish between "identified" and "identifiable." Only some of the FIPs will apply to identifiable information. This approach would give cloud companies an incentive to invest resources in maintaining information not as identified data, but in identifiable or even nonidentifiable form. Cloud companies would benefit from FIPs that become easier to meet as they move away from identified information. Individuals would benefit because security threats and other risks from identifiable data are, at least as a general matter, lower than from identified data.

"Automated processing" raises a problem analogous to that with the definition of "monitoring" in the context of jurisdiction. As I have noted, the Proposed Regulation would extend "jurisdiction" when there is a "monitoring of the[] behaviour" of data subjects.[168] I have argued above, however, that this term should not be applied indiscriminately to any use of networked intelligence to tailor services. As for "automated processing,"

---

165 *Id.* at 1880. On the importance of enforcement interests, see Schwartz, *supra* note 62, at 1677-79. For a discussion of the historical background of and variations in FIPs, see Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1969-79 (2013).

166 Schwartz & Solove, *supra* note 114, at 1881.

167 *Id.* at 1878.

168 *See supra* note 110 and accompanying text.

here, too, the cloud permits computing intelligence to be located on the network and to make choices without human intervention. A simple example, and one generally unproblematic from a privacy perspective, is a company's use of computer algorithms to monitor workload and distribute customer calls in real time among global call centers.[169]

The law should be concerned with risk based on decisionmaking with personal data rather than the mere automation of processing choices. More specifically, in a number of cloud service models, such as PaaS and IaaS, a cloud provider may not make decisions about the individuals whose personal data it is processing. In PaaS, the client has control over the deployed applications. IaaS involves a customer renting and using external computing resources, including operating systems and applications. In these cloud service models, the law generally should shift responsibility for information privacy from the cloud provider to its client.

Here, the test should be whether the cloud provider is a "mere conduit" for the client's data processing. As we have seen, the eCommerce Directive provides a test for deciding when intermediary service providers should be free from liability. Under the Directive, an entity that merely transmits information is not liable so long as it "does not initiate," "select the receiver of," or "select or modify the information contained in transmission."[170] These are useful inquiries for evaluating when a cloud provider who is merely offering computing from an outlet should be free of information privacy responsibilities.

In the case of SaaS, the analysis is more complex. Here, the cloud provider may make decisions based on the personal information of the individual whose information it processes. As an example, it may serve targeted ads to individuals who use web-based email services. The focus should be on having processes in place that are commensurate with the dangers raised by automatic decisionmaking. In some instances, the risk may be nonexistent or trivial; in others, it may be substantial.

Within the context of SaaS, more complex issues are raised when a company combines personal information from different cloud services. EU data protection authorities have already raised objections to Google's unified privacy policy, which took effect in March 2012. The policy permits Google to combine user data from its different services, including Google Apps,

169 *See supra* text accompanying notes 28-34.

170 eCommerce Directive, *supra* note 161, art. 12(1)(a)–(c), at 12.

such as Gmail and Google Docs, with data from its consumer services, such as YouTube and Google+.[171]

According to EU data protection authorities, Google's new privacy policy fails to provide clear information to users and engages in an "uncontrolled combination of data across services."[172] On the transparency point, the Article 29 Working Party, in an investigation led by the French data protection commission, found that the current policy does not permit a user "to determine which categories of personal data are processed . . . and the exact purposes for which these data are processed."[173] Regarding the sharing across different services, the EU data protection authorities found, "The new Privacy Policy allows Google to combine almost any data from any services for any purposes."[174]

In response, Google pointed to its use of "contextual in-product notices, in conjunction along with [its] overarching Privacy Policy."[175] In Google's view, the key test was "the totality of the information Google provides its users and how [it] delivers it."[176] Google also pointed to the benefits of giving users "easy access to their data across Google products" to allow "them to do useful things."[177] Moreover, it noted that users were still able to use its search product and YouTube without a Google account.[178]

The Google–European Union privacy collision is one of the clearest conflicts yet between U.S. and EU concepts of privacy. Google's strongest argument to the EU regulators concerns transparency. It is indeed difficult to make privacy notices both concise (which encourages readership) and comprehensive.[179] As for the combination of data, from the EU's perspective,

---

171 *See Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Oct. 16, 2012), http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser (criticizing Google's new privacy policy as providing "insufficient information" and control to users).

172 *Id.*

173 *Id.*

174 Letter from Article 29 Data Protection Working Party to Mr. Page 2 (Oct. 16, 2012), *available at* http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf. For Google's privacy policy, see *Policy & Principles: Privacy Policy*, GOOGLE, http://www.google.fr/intl/en/policies/privacy (last modified July 27, 2012). For a criticism of Google's single privacy policy and its consolidation of the information it collects, see Pamela Jones Harbour, Op-Ed., *The Emperor of All Identities*, N.Y. TIMES, Dec. 19, 2012, at A35.

175 Letter from Peter Fleischer, Global Privacy Counsel, Google, to Isabelle Falque-Pierrotin, Présidente, Commission Nationale de l'Informatique et des Libertés 2 (Apr. 5, 2012), *available at* http://assets.sbnation.com/assets/1045093/20120405_CNIL.pdf.

176 *Id.*

177 *Id.* at 3.

178 *Id.*

179 *See id.* at 1-2, 5.

Google has not made a strong argument simply by pointing to the usefulness of its services or the possibility of a consumer using its products, such as YouTube, without signing in to the service.

On April 2, 2013, the Article 29 Working Party completed its investigation of Google and finalized its findings of October 2012 regarding the insufficient aspects of that company's new privacy policy.[180] It declared that "Google has not implemented any significant compliance measures."[181] The locus of EU enforcement has now shifted to national data protection commissions, which will carry out additional investigations pursuant to their national legislation.[182]

Google's adoption of an opt-in approach tailored for each Google service would be an ideal first step toward solving this conflict. Requiring an opt-in for combining data will make the consent of a user more likely to be explicit and informed. In the mobile ad context, for example, Google has begun to ask users to verify their intentions to click on ads.[183] By requiring such intentionality, Google can increase the amount that it charges for mobile ads by demonstrating to the businesses that place ads with it that the end user's click was not merely the accidental tap of an errant finger.[184] Just as Google is willing to seek such verification to make mobile ads worth more to its advertisers and to its bottom line, it should strengthen the mechanisms of consent before permitting data to be combined across its services.

### C. *Contracts Plus*

Instead of reliance on supervised relationships within firms, the cloud makes possible a new use of the price system. In the context of the cloud, Coase's 1937 insights point to the conditions under which companies would shift from "make" to "buy" for networked computing services. Coase's *Nature of the Firm* predicts this result when the transaction costs of purchase,

---

180 *News: Google Privacy Policy: Six European Data Protection Authorities to Launch Coordinated and Simultaneous Enforcement Actions*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Apr. 2, 2013), http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo.

181 *Id.*

182 Eric Pfanner, *Google Faces More Inquiries in Europe Over Privacy Policy*, N.Y. TIMES, Apr. 3, 2013, at B4.

183 Claire Cain Miller, *Google Tries a Correction for "Fat Fingers,"* N.Y. TIMES, Dec. 17, 2012, at B7; *see also* Harbour, *supra* note 174 (expressing "concern[] about Google's dominant role in data collection").

184 *See* Miller, *supra* note 183 (noting that advertisers are paying less "for each click . . . in part because there are more mobile ads that are worth less").

including the negotiation of the necessary contracts, are less than the management costs of computing operations within the firm.[185]

Here, one can again contrast the EU and U.S. approaches. In the United States, the law of the cloud, at least for large corporations, is based primarily on contracts: for most consumers, it is the law of Terms of Service—that is, take-it-or-leave-it contracts.[186] In the European Union, the privacy framework, whether under the 1995 Directive or 2012 Proposed Regulation, does not permit the contracting out of basic obligations. In the language of contract law, EU data protection law creates immutable defaults. As Ian Ayres explains, as a general matter, while most legal rules can be changed through contract, there is a "smaller class of contract rules that parties cannot change by private agreement."[187] These rules are used when a "restriction on contractual freedom is needed to protect (1) parties within the contract, or (2) parties outside the contract."[188]

In the European Union, the privacy framework—whether that of the Directive or Proposed Regulation—limits the ability to contract out of basic obligations. This step protects both the parties within the agreement and those outside. As the Article 29 Working Party states, "[S]tandardised offers are a feature of many cloud computing services."[189] In its paper on the privacy implications of the cloud, the Working Party emphasizes the problem of information asymmetry between cloud providers and most clients. It finds a "specific risk[]" to be the "absence of transparency" to the client regarding how her personal data is processed.[190] Beyond the need to protect the parties within the contract, when businesses draft cloud agreements, they may not adequately protect the interests of third parties. The logic of EU law is that contracts, left alone, will be unable to manage the resulting privacy and security externalities for consumers.

Moreover, thus far the European Union has proceeded with standards rather than rules. Standards are more open-ended benchmarks, and rules are

185 *See* Coase, *supra* note 6, at 390-97.

186 On the weaknesses of reliance on such take-it-or-leave-it terms, see generally MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013).

187 Ian Ayres, *Default Rules for Incomplete Contracts*, *in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 585, 585 (Peter Newman ed., 1998).

188 *Id.* at 586.

189 Article 29 Data Prot. Working Party, *supra* note 21, at 8.

190 *Id.* at 5. The Working Party calls for the following policy in response: "Data subjects must be informed who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect." *Id.* at 2 (footnote omitted).

more hard-edged and fixed.[191] The European Union's mandatory obligations for privacy are written in FIPs at a high level of generality. This choice is wise due to the likely twists and turns of technological change. Yet the difficulty for the regulation of the cloud is that these general requirements are also accompanied by a labyrinth of murky doctrines, including those involving "controllers" and "processors."[192]

A key objective for the European Union should be to cut through its current regulatory thicket. A first move would be to develop model contractual clauses for data security, transparency, and data quality regarding all information in the cloud. In this regard, an International Data Corporation Report, carried out for the European Commission, proposed the creation of "clear and harmonised principles about cloud service providers' accountability and liability."[193] It also sought "the development of a set of standardised contract terms in order to implement these principles" and called for the European Commission to "take the lead" in this process.[194]

In the United States, by contrast, the realm of the cloud is largely contractual, with only limited legal requirements. In the future, more specific regulation can be expected regarding the content of cloud contracts. At present, the leading cloud regulations in the United States are state laws with obligations for data security, data breach security notification, and data disposal.[195] Through these laws, California and other privacy first movers at the state level are creating a requirement of reasonable security when personal data are processed.[196] In addition, applicable federal statutes in the healthcare and financial service sectors already provide more specific rules regarding the safeguards that must be in place when personal information is processed, including when it is processed in the cloud.[197]

---

191 For a discussion of rules and standards in the context of voting technology, see Paul M. Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. REV. 625, 655-67 (2002).

192 The European Union also faces the challenge of keeping its provisions for individual consent from becoming a catch-all to permit any processing of personal data. Hence, the Proposed Regulation contains notable limits on consent, including forbidding its use to "provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller." *Proposed Data Protection Regulation*, *supra* note 4, recital 34, at 22.

193 DAVID BRADSHAW ET AL., INT'L DATA CORP. (IDC), QUANTITATIVE ESTIMATES OF THE DEMAND FOR CLOUD COMPUTING IN EUROPE AND THE LIKELY BARRIERS TO UPTAKE 65 (July 13, 2012), *available at* http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf.

194 *Id.*

195 *See* SOLOVE & SCHWARTZ, *supra* note 75, ch. 11 (reviewing state provisions).

196 *Cf. id.*

197 *See, e.g.*, FED. FIN. INSTS. EXAMINATION COUNCIL, OUTSOURCED CLOUD COMPUTING 3-4 (2012), *available at* http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf; Modifications to the HIPAA Privacy Rules Under the Health

For an illustration of the future of cloud contracts, one might consider the wide range of regulatory bodies, beyond legislatures, that are likely to introduce requirements regarding information privacy and data security. These requirements will, in turn, affect the permissibility of those contractual terms and norms that are generated only by the parties to those agreements. As in the European Union, the language will likely be general, and many of the standards immutable (or, as Ian Ayres explains, not subject to alteration through contract). Consider the important guidance of July 2012 from the Federal Financial Institutions Examination Council (FFIEC) on outsourced cloud computing activities: The FFIEC agencies, which include the Consumer Financial Protection Bureau, consider "cloud computing to be another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing."[198] It called on financial institutions that outsource cloud computing "to consider the fundamentals of risk and risk management." [199] The resulting obligations for cloud contracts from the FFIEC start with privacy and data security.[200] Yet the FFIEC also requires financial institutions to engage in due diligence review, careful vendor management, ongoing audits, information security, business continuity planning, and "clear identif[ication] and mitigat[ion of] legal, regulatory, and reputational risks."[201] This language identifies a sweeping set of elements to be included in cloud contracts.

The analysis is different, however, for consumers who seek to contract directly for cloud services. There are significant differences in information available to the parties about critical service issues and how personal information is used. There are also important differences in market power in these business-to-consumer relationships. In that context, cloud contracts enter the realm of one-sided "Terms of Services." In the United States, a model law addressing cloud contract privacy would be helpful in providing a core baseline of protections.

---

Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

198 FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 197, at 1.

199 *Id.*

200 *Id.* at 2-4. As the FFIEC states, "Contracts with the cloud-computing service providers should specify the servicers' obligations with respect to the financial institutions' responsibilities for compliance with privacy laws, for responding to and reporting about security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches." *Id.* at 4.

201 *Id.* at 4.

## CONCLUSION

Cloud computing represents an important transformation for personal information processing. It has made international data transmissions into frequent occurrences, altered these data flows into multidirectional events, and allowed companies to purchase computing power and software as needed. These changes have created challenges to existing legal paradigms, and this Article has developed a series of proposals in response.

This Article began by looking at EU regulations that might make all cloud services used by an EU resident subject to EU data protection law. The Article has proposed modifications to the applicable EU jurisdictional law and, in particular, to the sweeping rules of the Proposed Draft Regulation. This Article's proposed test will cover entities "directing" their cloud activities toward the European Union, or where activities of EU citizens are "monitored" in the cloud in a fashion that raises privacy risks. Finally, the Article has recommended that EU law exempt from its general grant of privacy jurisdiction those cloud activities where data are only in transit.

Second, this Article considered the mismatch between the cloud and the respective statutory definitions of "personal information" in the European Union and the United States. Privacy law should not extend uniformly to all "identifiable" information, as it does in the European Union, and should not be limited to information that currently identifies an individual, as it tends to do in the United States. This Article drew on the Schwartz-Solove concept of PII 2.0 and argued that the law should not view all FIPs as applying to identifiable data. Here, the FIPs that are relevant apply to data security, transparency, and data quality. If applied to the cloud, the concept of PII 2.0 would create an incentive for cloud companies to maintain information not as identified personal information, but in an identifiable or even nonidentifiable form. As a related matter, the problematic concept of "automated processing" in EU law blocks exclusively machine-driven decisionmaking about persons. The current EU definition of this idea sweeps too broadly and prevents activities that are unproblematic from a privacy perspective. As a consequence, lawmakers should narrow the concept of "automated processing."

Finally, the cloud marks a rise in firms' purchasing of computer services rather than internally incorporating such capacity within their corporate structure. As a consequence, the legal realm of the cloud relies heavily on contracts between entities. In the European Union, the privacy framework seeks to limit the ability of parties to contract out of basic obligations. This approach can heighten protections of third parties. Greater standardization of terms is needed in the European Union to simplify the current regulatory

thicket around complex terms, such as "controller" and "processor." These concepts are not useful when applied to cloud arrangements. In the United States, state laws, such as those for data security breach notification, and data disposal, have begun to place some substantive limits that apply regardless of contract. Further regulatory obligations can be expected to continue to narrow the realm left exclusively to contractual obligations. There is also a need for a model contract privacy law that would provide a core baseline of protections in business-to-consumer arrangements. These suggested reforms will promote strong and effective protection for information privacy and also permit the cloud to become a central part of the evolving Internet.