Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU

Kevin McGillivray*

I. INTRODUCTION

Outsourcing has become an important tool for many businesses in the race to stay competitive and cost-effective. Information and communications technology has long been at the forefront of outsourcing on a national and international basis. This is largely due to the flexibility,

* © 2014 Kevin McGillivray. Doctoral Fellow, Norwegian Research Center for Computers and Law (NRCCL), Department of Private Law, University of Oslo (UiO). E-mail: kevin.mcgillivray@jus.uio.no. The author would like to thank Professor Lee A. Bygrave, Professor Knut Kaasen, Samson Esayas, and Francis Augusto Medeiros for their valuable comments on earlier drafts of this Article. This Article was written, in part, while working on the Confidential and Compliant Clouds (Coco Cloud) EU research project. COCO CLOUD, http://www.coco-cloud.eu (last visited Nov. 5, 2014).

broad application, and rapid growth of the computing industry. The latest evolution in information and technology outsourcing is so-called "cloud computing."[1] At its core, cloud computing is a method of providing users with on-demand computing services over a network.[2] Cloud computing provides users access to a variety of services including storage, use of software, and an array of applications.[3] Cloud computing allows businesses, governments, and consumers to outsource their computing needs in an efficient and cost-effective manner.[4]

The positive aspects offered by cloud computing services are numerous. Worldwide access to documents, inexpensive data backup, and access to new and innovative technologies all make cloud computing an attractive proposition.[5] Although cloud computing certainly has advantages, the creation of one-size-fits-all computing services raises many novel legal questions. Migrating data or services to the cloud is more than just a technical exercise—it is also a process with legal implications.[6] Cloud computing technologies and the law intersect in many areas, including consumer protection, intellectual property, data protection, and contract law, to name a few. In addition to technical systems that make cloud computing possible, cloud computing services are bound together by various legal instruments including contracts, privacy policies, and codes of conduct.

This Article evaluates the current legal and compliance issues in the use of cloud computing services in the European Union (EU). In addition to the application of data protection laws to cloud services, this Article evaluates the role of contracts and other methods of private ordering as a process or system of organizing and governing cloud computing. Specifically, the Article considers how contracts are used to manage or cope with potential conflicts between local, national, and international laws.

---

1. Andrew Joint & Edwin Baker, *Knowing the Past To Understand the Present—Issues in the Contracting for Cloud Based Services*, 27 COMP. L. & SEC. REV. 407, 408-09 (2011).

2. Christopher Yoo, *The Changing Patterns of Internet Usage*, 63 FED. COMM. L.J. 67, 83 (2010).

3. PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800–145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3 (2011).

4. Regina M. Faulkenberry, *Reviewing and Negotiating Cloud Computing Vendor Contracts*, 6 J. HEALTH & LIFE SCI. L. 119, 121 (2013). Popular services like Dropbox, Gmail, and iCloud are common examples of cloud computing services.

5. *See* Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 325 (2013) (arguing that cloud computing is more than a "buzzword").

6. Alberto G. Araiza, *Electronic Discovery in the Cloud*, 2011 DUKE L. & TECH. REV. 8, 12-13 (2011).

More concretely, I consider the contractual compliance requirements of EU data protection laws (EU DPL) and evaluate how these requirements intersect with contracting practices commonly used in cloud computing. Is the current use of private ordering to regulate cloud computing by contract or other means sufficient to comply with EU DPL? In other words, is the current level of state participation and regulation adequate or should states take a greater role? To make this determination, this Article considers regulations currently in force, as well as planned or future methods of regulation. This evaluation focuses primarily on the terms of several "public cloud" agreements, which have been widely deployed on a global scale.[7]

The Article is divided into three main Parts. The first Part considers current definitions of cloud computing and provides a brief overview of the technology and industry. The second Part outlines the role that contracts play in cloud computing and explains the present contracting practices and structure of cloud computing services. Part II further considers how the structure and organization of the agreements impact cloud consumers and affect their ability to exercise rights they may have pursuant to the laws of their home jurisdictions. The third Part considers the intersection of contract terms and EU DPL. Finally, Part III considers how contracts aimed at a global audience fit into national regulatory models, principally in the EU.

A. Computing on a Cloud

To make cloud computing possible, several existing technologies have been combined and are now being employed on a global scale. These technologies are used to manage many computers, sometimes millions of them, remotely over the Internet. This method of remote computing has been deemed the "next big idea" in technology, even if the idea is not entirely new.[8]

On the cloud, data is available anywhere at any time and is accessible with multiple devices. Improved networks and greater access to broadband Internet has made it possible for consumers and businesses to do much more of their computing remotely, reducing the need for powerful personal computers.[9] Cloud computing takes place on

---

7. MELL & GRANCE, *supra* note 3, at 3.

8. Jasper Sluijs et al., *Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market*, 3 J. INTELL. PROP., INFO. TECH. & E-COMMERCE L. 12, 12 (2011).

9. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1198-99 (2010).

machines that the cloud consumer does not own, often with software they do not have to purchase, download, or even update. Cloud computing users store everything from valuable commercial data to family photographs on servers over which they have little or no control.[10] These servers are placed in physical locations the user will likely never visit and may even have trouble finding on a map.[11]

Many cloud users are unaware that they are using a cloud computing service.[12] The term "cloud computing" has proven to be an extremely effective metaphor.[13] Commercials created by cloud service providers (CSPs) show cluttered files being whisked away to a brighter, fluffier place, where organization and security reign. In reality, moving to the cloud is, of course, more complicated and less idyllic than the commercials let on, at least from a legal point of view. Relocating to the cloud often entails transferring personal data to remote servers, which must be placed somewhere.[14] The location could be down the street, across the globe, or in both places at the same time. From a technical perspective, the location of the users' data is irrelevant, although the location of personal data has legal implications.[15]

B. Advantages of Cloud Computing

Unlike traditional IT outsourcing, which was primarily used by "big players" including large businesses, cloud computing is being adopted widely by small- and medium-sized enterprises (SMEs), consumers, and governments at all levels. In the United States, the federal government is pursuing a "cloud first" strategy and is incorporating large public cloud

---

10. *See* Cindy Pham, *E-Discovery in the Cloud Era: What's a Litigant To Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 144-45 (2013); Tom Vanderbilt, *Data Center Overload*, N.Y. TIMES (June 8, 2009), http://www.nytimes.com/2009/06/14/magazine/14search-t.html?pagewanted=all.

11. Adam W. Snukal et al., *Cloud Computing—Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing, Part One*, 65 CONSUMER FIN. L.Q. REP. 57, 58-59 (2011).

12. *See* Wakefield Research, *Citrix Cloud Survey Guide*, CITRIX 1 (Aug. 2012), http://www.citrix.com/content/dam/citrix/en_us/documents/go/wakefield-citrix-cloud-survery-guide.pdf?accessmode=direc ("The majority of Americans (54%) claim to never use the cloud, however 95% of those who think they're not using the cloud, actually are.").

13. Mihály J. Ficsor, *The WIPO "Internet Treaties" and Copyright in the "Cloud,"* ALAI 2012 CONGRESS KYOTO 1-2 (2012), http://www.alai.jp/ALAI2012/program/paper/The%20WIPO%20Internet%20Treaties%20and%20copyright%20in%20the%20Cloud%20%EF%BC%88Dr.%20Mih%C3%A1ly%20J.%20Ficsor%EF%BC%89.pdf.

14. Snukal et al., *supra* note 11, at 58-59; Araiza, *supra* note 6, at 10. Major cloud providers are contemplating locating data centers in "Siberia, abandoned coalmines, and on ships at sea." *Id.*

15. Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 23-24 (2010).

providers to meet its computing needs.[16] In the United Kingdom, governments have embraced cloud computing and are moving services to a "G-Cloud" to meet government computing requirements.[17] Many nations are following this trend.[18] As a result of broad cuts and reduced tax revenues, many state and local governments are also finding cloud computing more attractive. City governments from Los Angeles, California, to Narvik, Norway, have started using Google Applications rather than producing the services in house or purchasing traditional IT solutions.

Although strained budgets and cost saving measures may be at the center of this rush to take up cloud computing for some users, the benefits often go beyond lower IT costs.[19] Cloud consumers now have the opportunity to purchase services, on a worldwide basis, that are limited or scalable to their individual needs.[20] For businesses, the costs of cloud-based services are often lower than traditional IT outsourcing.[21] Cutting-edge computer programs, once reserved for the largest corporations, have become widely available to SMEs. In addition to greater choice, security may also be improved. Both consumers and commercial users of cloud computing only pay for the computing power they use, reducing wasted processing capacity.[22] In many cases, cloud computing services are available free of charge to cloud consumers who are willing to share their personal information.[23] In addition to productivity and cost benefits, cloud computing is argued to be more environmentally friendly or "greener" than traditional computing.[24]

---

16. Vivek Kundra, Exec. Office of the President of the U.S., *Federal Cloud Computing Strategy*, CTO.GOV 2 (Feb. 8, 2011), http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

17. CHRISTOPHER MILLARD, CLOUD COMPUTING LAW 108-09 (2013).

18. *See* Urs Gasser & David R. O'Brien, *Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*, SSRN (Mar. 17, 2014), http://ssrn.com/abstract=2410270 (select "Download This Paper") (discussing government cloud strategies in the United States, United Kingdom, EU, and Japan); John Herhalt & Ken Cochrane, *Exploring the Cloud: A Global Study of Governments' Adoption of Cloud*, KPMG (2012), http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/Exploring-the-Cloud.pdf.

19. Gasser & O'Brien, *supra* note 18, at 6-7. Although this may not be the primary reason, the U.S. government estimates a savings of $5-12 billion on a yearly basis, while the U.K. government expects to save "£40M during 2013-2014, and £120M during 2014-2015."

20. *See, e.g.*, Joseph A. Nicholson, *Plus Ultra: Third-Party Preservation in a Cloud Computing Paradigm*, 8 HASTINGS BUS. L.J. 191, 199 (2012).

21. *Id.* at 199-200.

22. Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. TELECOMM. & HIGH TECH. L. 53, 64 (2011).

23. Robison, *supra* note 9, at 1214.

24. Rob Bernard, *The Cloud's Green Advantage*, FORBES (Nov. 15, 2010, 6:00 AM), http://www.forbes.com/2010/11/12/energy-datacenter-enterprise-technology-cloud.html.

Though an interconnected world of data brings many positive features, new problems or challenges have also arisen. Increased use of shared infrastructure, accessible on a worldwide basis, has created challenges for users and regulators—particularly in the areas of intellectual property, data protection, or data privacy—and regulatory compliance in many individual sectors such as finance and healthcare.[25] As long as the services functioned properly, there were few that gained public interest. However, revelations of government access to cloud consumer data, profiling by companies, and large-scale infringement have all brought attention to the use of cloud computing.[26] Courts attempting to apply old rules to cloud technologies have encountered some difficulty.[27]

C. Defining Cloud Computing

There is no standard legal definition of cloud computing.[28] Cloud computing is used to describe a method of computing that combines old and new computing technologies.[29] One of the most commonly referenced definitions of cloud computing in both the EU and the United States was created by the National Institute of Standards and Technology (NIST), a part of the United States Department of Commerce (DoC).[30] The NIST defines cloud computing: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider

---

25. Gervais & Hyndman, *supra* note 22, at 71.

26. *See* Judith Rauhofer & Caspar Bowden, *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* 11-12 (Edinburgh School of Law Working Paper No. 2013/28, 2013) (discussing the U.S. surveillance program "PRISM").

27. Gervais & Hyndman, *supra* note 22, at 71.

28. *See* Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1812-13 (2011); Joseph A. Schoorl, *Clicking the "Export Button": Cloud Data Storage and US Dual-Use Export Controls*, 80 GEO. WASH. L. REV. 632, 644 (2012).

29. Sluijs et al., *supra* note 8, at 13-14.

30. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, EUROPEAN COMMISSION 27 (July 1, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. The Article 29 Working Party (WP29) is made up of a representative from the data protection authority of each EU Member State. WP29's opinions are advisory only. *See also* Peter Hustinx, *Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe,"* EUR. DATA PROTECTION SUPERVISOR ¶ 4 (Nov. 16, 2012), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

interaction."[31] Cloud computing provides a service such as data storage, use of software, and an array of applications, rather than a tangible good.[32] There remains a lack of uniformity in the terms used to reference different parties to cloud computing services in different jurisdictions. In this Article, the final end user of a cloud computing service, whether it is a consumer, government, or business will be deemed a "cloud consumer."[33] CSPs will be used to describe the party making a cloud service available. Because many CSPs use cloud computing services themselves, referencing only the "user" provides an incomplete picture of the final end user.[34]

D. Cloud Service Models

The amount of control the cloud consumer or the CSP has over their data depends in part on the cloud model being offered. Depending on the needs of the user, there are three general service models available:

1) Infrastructure as a Service (IaaS) provides the cloud consumer with computing resources such as processing power and/or storage used by businesses, consumers, and other cloud service providers.[35] Under this model, the user has control over the applications or information that is put onto the cloud. Cloud consumers essentially rent the space they need.[36]
2) Platform as a Service (PaaS)—software for constructing (and usually deploying) custom applications.[37]
3) Software as a Service (SaaS) provides the end user with access to software and other computing resources.[38] Under this model, the user has the least amount of control. The cloud consumer does not

---

31. Mell & Grance, *supra* note 3, at 7.

32. Angela Adrian, *How Much Privacy Do Clouds Provide? The Future of Privacy Regulation in an Online World*, *in* CONTEMPORARY PRIVATE LAW 158, 159-60 (defining cloud computing as a service rather than a product); MILLARD, *supra* note 17, at 331-61.

33. FANG LIU ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 500-292, NIST CLOUD COMPUTING REFERENCE ARCHITECTURE 5-6 (2011).

34. In the EU, the end user of a cloud service is sometimes deemed a "cloud client." *See, e.g.*, Rhonda Farrell, *Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme*, 19 INFO. SEC. J.: A GLOBAL PERSP. 310, 312 (2010).

35. Lutz Schubert, *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*, *in* EUROPEAN COMMISSION ON INFORMATION SOCIETY AND MEDIA 9-10 (Keith Jeffery & Burkhard Neidecker-Lutz eds., 2010).

36. John Soma et al., *Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services*, 16 J. TECH. L. & POL'Y 193, 198-99 (2011).

37. *Id.* PaaS examples include Force.com, Google App Engine, and Windows Azure (Platform).

38. *Id.* SaaS examples include Google Docs, Salesforce CRM, and SAP Business by Design.

control software, applications, or storage used to perform their computing functions.

Lines between the these above-referenced services are not always clear. Some CSPs provide a mixture of services that incorporate overlapping aspects. CSPs may also be users of other cloud services themselves. For example, a CSP offering software as a service may not have its own server infrastructure. In that case, the SaaS provider will be a cloud consumer of IaaS. The end user signing up for the SaaS product will essentially be using more than one type of cloud service.[39]

In addition to different service models, not all clouds are created with equal accessibility. Currently, there are several primary models of cloud computing including "private," "public," and "hybrid" clouds.[40] On the most secure side of the spectrum, private clouds are often dedicated to a single organization or shared by members of the same corporate group.[41] "Community clouds" are similar to private clouds in that they have controlled access and limit the parties that may access the computing resources. Instead of being limited to a single company, the community can include several actors or organizations with similar processing needs. An example might be a "financial cloud," "banking cloud," or even a healthcare cloud.[42]

On the less secure side of the spectrum, "public clouds," like those provided by Amazon and Google, provide access to many users, often through the use of large data centers.[43] Public clouds are considered to be the least secure and personal data may be more readily monitored for "secondary uses" or reused by third-party applications for advertising

---

39. MILLARD, *supra* note 17, at 13-14 ("[U]sers may not necessarily know how a cloud service has been put together or who supplies, provides, or operates different components."); Susan A. Berson, *Safe in the Cloud? Online Service Risks Need Care and Coverage*, ABA J. (Nov. 1, 2011), http://www.abajournal.com/magazine/article/safe_in_the_cloud_online_service_risks_need_care_and_coverage/.

40. *See, e.g.*, Anne C. Datesh, *Storms Brewing in the Cloud: Why Copyright Law Will Have To Adapt to the Future of Web 2.0*, 40 AM. INTELL. PROP. L. ASS'N Q.J. 685, 690 (2012).

41. M. Auty et al., *Inadequacies of Current Risk Controls for the Cloud*, 2ND IEEE INT'L CONF. ON CLOUD COMPUTING TECH. & SCI. 659 (2010), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5708515&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5708515.

42. John W. Hill et al., *A Proposed National Health Information Network Architecture and Complementary Federal Preemption of State Health Information Privacy Laws*, 48 AM. BUS. L.J. 503, 548 (2011).

43. David Lametti, *The Cloud: Boundless Digital Potential or Enclosure 3.0?*, 17 VA. J.L. & TECH. 190, 210-11 (2012) (stating that "public clouds" are privately held companies and are not "public" in the general use of the term or run by governments, but public in that they are widely accessible).

purposes.[44] As a result of their size and design, it may be difficult for providers to determine where data is being stored at any given time in the public cloud.[45]

II. CONTRACTUAL STRUCTURE USED IN CLOUD COMPUTING

Like other commercial offerings, contracts play an important role as a means of organizing and defining the legal associations created in cloud computing services.[46] In addition to defining relationships with customers and other providers, contracts are used by CSPs as a tool for managing risk and liability.[47] Contract terms allow CSPs to clearly manifest their expectations and requirements throughout the period of the service. Contract terms generally include technical and performance requirements in addition to the duration of the service, the price, and the methods for terminating the agreement. The terms offered in cloud computing contracts are often provided on a take-it-or-leave-it basis, although some customers are able to obtain customized agreements through negotiation.[48]

Contracts also play an essential role in facing the many regulatory challenges created by the uneven and in some cases unpredictable regulatory structures facing CSPs.[49] As noted in one study:

> In the cloud context, *contracts* have played a particularly important role in embracing (and absorbing) some of the challenges associated with the technological innovation. In the first phase, cloud providers and customers have addressed core issues using contractual agreements to identify and allocate risks and responsibilities and create enforcement mechanisms where existing rules are inadequate.[50]

In addition to expectations and compliance needs, contract terms often define the remedies available in the event that the service malfunctions.

---

44. Faulkenberry, *supra* note 4, at 150-51.

45. Juliette Garside, *How Global Laws Protect Your Data*, GUARDIAN (Oct. 16, 2011), http://www.theguardian.com/cloud-technology/global-laws-protect-your-data.

46. NEW STUDIES IN GLOBAL IT AND BUSINESS SERVICE OUTSOURCING: 5TH GLOBAL SOURCING WORKSHOP 2011: COURCHEVEL, FRANCE, MARCH 14-17: 2011 REVISED SELECTED PAPERS 48 (Julia Kotlarsky et al. eds., 2011).

47. EMILY M. WEITZENBOECK, A LEGAL FRAMEWORK FOR EMERGING BUSINESS MODELS DYNAMIC NETWORKS AS COLLABORATIVE CONTRACTS 150 (2012).

48. MILLARD, *supra* note 17, at 73-107.

49. Sluijs et al., *supra* note 8, at 26-27.

50. *See* Urs Gasser, Berkman Ctr. for Internet & Soc'y, Harvard Univ., *Cloud Innovation and the Law: Issues, Approaches, and Interplay*, SSRN (Mar. 17, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410271 (providing that a second phase where best practice models will be used to "legally embrace" the effects of cloud innovation. Technical measures are also being developed that will likely play an important role in this second (or potential third phase)).

Along with mapping responsibilities throughout the lifecycle of the service, cloud computing contracts often dictate the forum where cloud consumers may pursue remedies against their CSP and the law to be applied in the event of a dispute. The contract agreed upon between the CSP and the cloud consumer acts as the "law" governing the parties' legal relationship. Subject to some limitations, parties to the contracts are free to agree to a wide variety of terms.

The law agreed to between or among the parties to a contract does not exist alone. External constraints, such as national laws or international agreements, impact the validity and enforceability of contract terms. Although contracts will explicitly govern many aspects of the parties' relationship, national laws such as data protection laws may be in conflict with contract terms. In cloud computing, it is possible to have several sets of national laws applicable at the same time, particularly in areas of law with extraterritorial application.[51] Conflicts between and among domestic or national laws often take place without a clear path to deal with the conflicts.[52] For example, there is no international cloud computing treaty. Global contracts are drafted, to some extent, to meet this trans-border challenge. However, contracts drafted for globally accessible cloud services are still subject to local speed limits in many respects. In this Part, some of those speed signs, and CSP's ability or willingness to brake for them, are examined.

The notion that parties use contracts to regulate conduct and to define legal relationships is not a new phenomenon nor is it unique to cloud computing.[53] Traditional contract rules are being applied to this new technology, much like they have been applied to other emerging technologies in the past. This Article does not maintain that cloud computing has turned contracting on its head to such an extent that completely new contracting rules or methods must be created. However, based on the organization, internationalization, and application of cloud computing services, the contracts do have novel aspects when compared with more traditional IT outsourcing contracts. Although it can be

---

51. *See, e.g.*, DAN JERKER B. SVANTESSON, EXTRATERRITORIALITY IN DATA PRIVACY LAW (2013).

52. Moreover, a party to a cloud computing contract may face the situation where compliance with the terms of the agreement means noncompliance with the national laws in one of the jurisdictions where their service operates, resulting in fines or fees. Conversely, following national legislation may mean breaching an agreement with a partner or subcontractor—resulting in contractual liability. *See* Fabrizio Cafaggi, *The Regulatory Functions of Transnational Commercial Contracts: New Architectures*, 36 FORDHAM INT'L L.J. 1557, 1601-02 (2013) (examining this situation in transnational contracts).

53. WEITZENBOECK, *supra* note 47, at 157.

argued that there is nothing new under the sun when it comes to application of contracts, the cloud is making things cloudier.

A. Contracting onto the Cloud

CSPs enter into contracts with cloud consumers in a number of ways. For some cloud consumers, the agreements follow the traditional contracting scheme and are reduced to paper, but most users agree to terms electronically.[54] Although electronic contracts may raise issues regarding the law applicable to the formation of the contract, the electronic nature of an agreement does not generally impact its validity.[55] An electronic contract that is validly formed online will generally be enforceable.[56]

For many public cloud users, cloud consumers simply "click-through" a set of standard terms that will enable them to access the CSP's service.[57] The so-called "click-wrap" terms are often long, full of technical and legal language, and written in a manner difficult for many users to comprehend, particularly consumers and unsophisticated SMEs.[58] Clicking on an "accept" or "agree" button forms a valid contract wherein many pages of terms and conditions are incorporated.[59] For the cloud consumer, their entry point onto the cloud and their access to its many offerings is through their contract with the CSP. Terms agreed to between the parties at this stage form the basis and set the standard for the entire use of the cloud service. This contract defines the actions the CSP may take, in addition to any limitations or obligations the cloud consumer may have. The contract covers issues relevant for use of the service including intellectual property rights, choice of law or forum, indemnification, and liability, among others.[60]

---

54. Mark Allen Chen, *Interactive Contracting in Social Networks*, 97 CORNELL L. REV. 1533, 1537-40 (2012).

55. *E.g.*, Dawn Davidson, *Click and Commit: What Terms Are Users Bound to When They Enter Web Sites?*, 26 WM. MITCHELL L. REV. 1171, 1178-79 (2000).

56. Sebastian Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 451, 454 (2012) (defining a valid agreement for contracts as containing an offer, acceptance, mutual assent, and consideration).

57. *See, e.g.*, Michael J. Brito, *Cloud Computing, Multi-Sourcing Create New Challenges in Outsourcing*, *in* INSIDE THE MINDS: BEST PRACTICES FOR MANAGING OUTSOURCING TRANSACTIONS 151 (2014), *available at* 2014 WL 1600655.

58. Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 1 (2014). In one study, it was determined that if average U.S. readers read each of the privacy policies they were presented, it would amount to twenty-five days of reading the agreements each year.

59. *Id.* at 62.

60. Zimmeck, *supra* note 56, at 465 (discussing the application of "secondary privacy law" in areas where a contract is silent or not validly entered).

In addition to the free cloud computing services available to consumers and businesses, many are also available on a pay-for-use basis. In the case of paid services, CSPs often include service-level agreements (SLAs) that define specific requirements of the service such as price and availability in addition to any specifically negotiated terms.[61] Although paid services may provide cloud consumers with some guarantees, in the case of most cloud computing services, there is no opportunity for negotiation. In the case of high-value or strategically important contracts for CSPs, negotiation is more likely.[62]

For the majority of cloud users, whether SMEs or consumers, the reality is a standard service offered on click-wrap terms.[63] In accepting a standard contract, the cloud consumer often agrees to terms allowing their data and other information to be passed through a worldwide network, under the control of many loosely affiliated actors. From a general contractual point of view, if the cloud consumer is satisfied with the contract and guarantees provided by the CSP, there is no need to look any further at the contracting structure or consider how the service is delivered, including the role of subcontractors. The service just needs to work. However, with some compliance issues, such as EU DPL, the cloud consumer needs a greater level of transparency and an understanding of the system they are using. The cloud consumer's obligation under the general rules of contract may differ from their obligations under data protection law. The structure of many services, and the legal implications flowing from this structure, will be discussed in the following Subparts.

B. Organization of Contracts and Services

The cloud computing market is developing quickly, bringing with it many new market players. In addition to household names like Apple and Microsoft, many CSPs are startup companies with innovative ideas, but limited resources and infrastructure. By using the advantages of cloud computing, many startups are able to bring new ideas to the market with relatively low budgets.[64] To launch their services, CSPs often employ the resources of other providers—particularly storage

---

61. Araiza, *supra* note 6, at 12 ("[T]he data in data centers may be subject to foreign laws or no laws at all.").

62. Daniel Carmeli, *Keep an I on the Sky: E-Discovery Risks Forecasted for Apple's iCloud*, 2013 B.C. INTELL. PROP. & TECH. F. 1, 12 (2013).

63. Ellen Wauters, Eva Lievens & Peggy Valcke, *Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites*, 22 INT'L J.L. & INFO. TECH. 254, 255 (2014).

64. Sluijs et al., *supra* note 8, at 1125-28.

infrastructure from major providers like Amazon or Google.[65] If a startup service becomes popular, the provider needs the flexibility to expand and increase capacity, add storage space, change software, or simply to obtain more competitive prices from third parties on the services the CSP uses.[66] Similarly, if a provider in the supply chain goes out of business or no longer makes sense within the CSP's business model, the CSP needs to be able to adjust and add new partners. Contract terms reflect this market reality by allowing CSPs to change partners and add layers to the service on a flexible basis.[67]

The flexibility built into these contracts reflects the common situation that exists when a cloud service is being launched. That is, the CSP may not know the eventual size or structure of their network.[68] Cloud consumers are entering into a preexisting structure with contracts already in place.[69] Additionally, partners are often added or removed after the original contract is formed. From the perspective of the CSP, the fewer guarantees or limits to expansion it has in the contract, the more flexibility the CSP will have in dealing with future vendors and expansion down the road. Changes in terms, providers, and adding or removing parties are common, if not expected, occurrences in many cloud computing arrangements.

In addition to allowing liberal use of subcontractors, CSPs often reserve the right to subsequently amend the terms of the agreement without requiring further consent.[70] CSPs retain the right to unilaterally amend specific contractual terms for a variety of reasons. A contract may, for example, allow the CSP to implement new technology or react to regulatory changes. Some changes may be trivial and have no impact

---

65. Scott Bender, *Privacy in the Cloud Frontier: Abandoning the "Take It or Leave It" Approach*, 4 DREXEL L. REV. 487, 489 (2012) (maintaining that cloud computing infrastructure is almost exclusively privately owned and that Amazon Web Services, one of the largest cloud providers, is presumed to account for 1% of all Internet traffic); Didier Bigo et al., *Fighting Cybercrime and Protecting Privacy in the Cloud*, EUR. PARLIAMENT (Oct. 15, 2012), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf.

66. Neil Robinson et al., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, SSRN (Nov. 30, 2010), http://www.ssrn.com/abstract=2141970 ("[I]ndividual entities change roles quickly as personal data are moved, restructured and re-used continuously.").

67. MILLARD, *supra* note 17, at 89 ("Providers' terms generally entitle them to use sub-contractors, for example for support services.").

68. Hustinx, *supra* note 30, ¶ 6. Hustinx provides that complex contract questions "may be aggravated considerably when new providers can be added to the service dynamically during operation." *Id.*

69. MILLARD, *supra* note 17, at 31-32.

70. Wayne Jansen & Tim Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NAT'L INST. STANDARDS & TECH. 7-8 (2011), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

on the functionality or security of the service. Others may be major and may impact the cloud consumer's security or compliance needs.

Contracts that limit subcontracting, modification or variation of terms, or provide strict limits on the use of data are unusual in free services. Without reservations in the contract, subcontracting and sharing of personal data takes place with few limits—at least without breaching the contract. Whether this flexibility complies with certain data protection regimes is another issue that will be considered further in Part II.C.

C. Subcontracting Structure and Layers of the Cloud

The detached organizational structure of the cloud often results in long "chains" of primary, sub-, and sub-subcontractors.[71] The result is a collection of many actors taking part in operating different parts or layers of the cloud infrastructure.[72] These agreements may include software and storage providers, ISPs, or other network providers.[73] Although the term "partners" is often used in agreements, infrastructure and other providers are not necessarily under the same corporate or organizational umbrella. Their association or contractual relationship is often limited to individual agreements with the CSP. The situation is aptly described as a "complex mesh of contracts" that often provide few details regarding the treatment of the cloud consumers' data once it enters the "heavily subcontracted" cloud structure.[74] Furthermore, the parties change frequently, are often located in different countries, and are potentially governed by the laws of multiple jurisdictions at the same time.[75] The diagram below illustrates how a cloud transaction, on a small scale, might look.

---

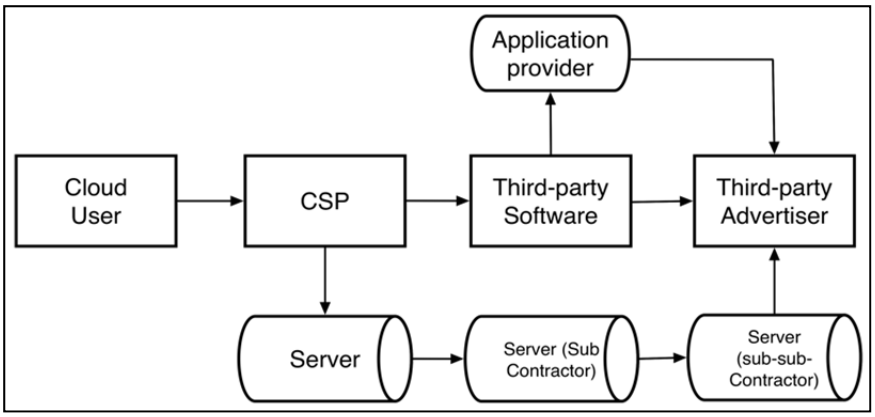
71. Isabell Conrad et al., *Cloud Computing Contracts—Discussion Paper on Subcontracting*, EUR. COMMISSION 3 (2014), http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion_paper_en.pdf ("Cloud Computing for Consumers and Small & Medium Enterprises . . . has become unthinkable without subcontracting.").

72. Sluijs et al., *supra* note 8, at 2012.

73. *Id.*

74. Bigo et al., *supra* note 65, at 12.

75. *See* Miranda Mowbray, *The Fog over the Grimpen Mire: Cloud Computing and the Law*, 6 SCRIPTED 132, 141 (2009); Bender, *supra* note 65, at 489; *see also* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1643-44 (2013) (arguing that the tests proposed in the draft EU data protection regulation (art. 3(2)) will greatly expand the EU's claim of jurisdiction over CSPs located outside the EU).



In the above graphic, the contract between the CSP and the cloud consumer does not generally contain information regarding partners or subcontracted parties that will provide core infrastructure used in the service—although it does contain terms allowing for such network. For example, the CSP may be outsourcing all of its storage to third parties located in countries outside of the cloud consumer's home jurisdiction and even the CSP's. Partners storing data on behalf of the CSP may further outsource storage to secondary data centers. The terms of the agreements between the CSP and its subcontractors may vary from those in the original agreement between the CSP and the cloud consumer, depending on the infrastructure and subcontractors selected by the CSP and the system used to include "back-to-back" terms. Although synchronizing terms in the agreements among all actors is difficult, data protection law in some jurisdictions requires it.[76]

If the cloud consumer is unaware of the scope of the contractual chain, evaluation of the agreements for compliance purposes is difficult.[77] At their initial entry point to the cloud—the contract with the CSP—the cloud consumer has likely authorized a transfer of their data to subcontractors or third parties with few limitations. However, the cloud consumer may not understand the breadth or the complexity of the structure, nor the ultimate location or use of their data.[78] Further, the

76. Robinson et al., *supra* note 66, at 134.

77. NIKOLAUS FORGÓ ET AL., CLOUD LEGAL GUIDELINES—FINAL REPORT 14 (2013) (finding that synchronizing the chain of agreements and enforcing contract terms against multiple actors becomes difficult in the cloud structure).

78. Peter Blume, *Controller and Processor: Is There a Risk of Confusion?*, 3 INT'L DATA PRIVACY L. 140, 142 (2013) ("[F]rom the viewpoint of data protection this model creates disturbing complexity and uncertainty."); *see also Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 17.

cloud consumer may also have limited appraisal of the risks inherent in the shared structure they are entering and which party bears the risk of loss if the service encounters problems.

There are many examples of the above scenario in the cloud. Apple's iCloud service initially stored data uploaded to its service on servers owned by Microsoft and Amazon.[79] Although Apple owned some of its infrastructure, its initial "public" iCloud service did not limit data storage to computers owned by Apple, even if this fact was not apparent from the iCloud contract terms.[80] A cloud consumer using the iCloud service is, therefore, not in a position to analyze the storage location or policies of third-party providers storing the cloud consumers' data.

The amount of information provided in cloud contracts is not uniform. Some major providers clarify physical location of data storage, but may not provide complete information on all parties to the service or strictly limit their roles. Like many other CSPs, the popular storage provider Dropbox does not own the servers where its end users store their information. A user of Dropbox is, however, able to obtain the following information about the placement or storage of their data:

> Once a file is added to your Dropbox, it's synced to Dropbox's secure online servers. All files stored online by Dropbox are encrypted and kept in secure storage servers. Storage servers are provided by a managed service provider, and an infrastructure is located in data centers across the United States.[81]

The end user is put on notice that their data will be moved to the United States after being encrypted. The user can also ascertain that Dropbox and Amazon have an agreement for the storage, although the terms for the storage are not made available to the cloud consumer. If Dropbox goes out of business, suffers a major security lapse, or has other problems, what can a cloud consumer expect or require of Amazon regarding their data? If a cloud consumer leaves the Dropbox service, will their data be deleted from all of Amazon's storage facilities? If Amazon can access the cloud consumer's personal data, what terms govern the use of the cloud consumer's data by Amazon's third-party software and application partners for behavioral advertising purposes? Does Amazon have a contractual duty to Dropbox users? Based on the contractual arrangement, it seems unlikely that Amazon has contractual

---

79. Carmeli, *supra* note 62, at 13-14.

80. *Id.*

81. *Where Does Dropbox Store Everyone's Data?*, DROPBOX, https://www.dropbox.com/help/7/en (last visited Oct. 25, 2014). Dropbox does not provide a separate contract or amended terms for users in the EU.

liability, although extracontractual claims are a possibility.[82] In the event of a loss, absent an additional contract with Amazon, the consumer's contractual remedy will likely have to come from Dropbox.

Many CSPs offer substantially less information regarding the parties involved in providing their cloud services. Evernote, a popular SaaS provider, provides the following standard term: "If you use the Service, you acknowledge that you may be sending electronic communications (including your *personal account information and Content*), through computer networks owned by Evernote and third parties located in California and other locations in the *United States and other countries*."[83] This term provides the end user with very little information regarding the ultimate location of the storage of their data. "Other countries" places no boundaries on the eventual location of the data. Moreover, what level of access will these third-party providers in "other countries" have?[84] Even providers that offer specific "zones" for data storage may not provide contractual guarantees that data will remain there.[85]

There are CSPs providing services focused on the European market that are more actively attempting to meet EU DPL requirements. For example, the CSP "CloudMe" uses its EU location in Sweden and its purported adherence to EU DPL as a selling point for its service in its advertisements. The terms of service provide that "(a)ll user data and data centers are located within the European Union."[86] However, like other CSPs, CloudMe interacts with providers in the international market. Although the contact terms advertise compliance with EU laws, the contract contains exceptions that may result in some information being provided beyond a limited geographical region. CloudMe's terms provide some limited but important exceptions to keeping data in conformity with EU laws.

> Solutions that are owned by American companies or stored in solutions owned by American companies falls [sic] under US legislation (such as

82. *See, e.g.*, Robert H. Carpenter, Jr., *Walking from Cloud to Cloud: The Portability Issue in Cloud Computing*, 6 WASH. J.L., TECH. & ARTS 1, 3-4 (2010).

83. *Terms of Service*, EVERNOTE (Oct. 5, 2014, 10:30 PM), http://evernote.com/legal/tos.php (emphasis added).

84. Faulkenberry, *supra* note 4, at 26. For cloud consumers, the use of the cloud can potentially increase the number of "contacts" a party is found to have for personal jurisdiction purposes.

85. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 54 (discussing Amazon TOC on zone storage); MILLARD, *supra* note 17, at 55 (providing that Amazon's "zone storage" is not contained in its contract terms).

86. *Legal and Terms of Service*, CLOUDME, https://www.cloudme.com/en/legal (last visited Oct. 25, 2014).

> The Patriot Act and the proposed SOPA) and can therefore at any time be judged to hand out any form of information to US authorities about the users of the service or the content stored.[87]

Depending on the solutions used, the disclosure of user information outside of the EU could be extremely broad, despite the promises of EU law compliance and storage in Sweden.

D. User Concerns and Risks of the Multilayered Cloud Contracting Structure

Cloud computing users place valuable information in a shared infrastructure and surrender a great deal of control over their data to third parties. Many of the risks associated with cloud computing relate to security, availability, and integrity of data.[88] The risks associated with the multilayered cloud computing structure vary depending on the solution used (SaaS, PaaS, IaaS, etc.) and the type of data being stored. Similarly, the level of access CSPs will have to customer data varies depending on the service. Depending on factors like encryption, location of subcontractors, and the nature of the information being stored on the cloud, cloud consumers face different levels of risk.[89] Common concerns of cloud computing users largely revolve around the ability to access their data, unexpected losses of data, and the inability to restrict other parties from accessing information they store on the cloud.

In public cloud models, data moves across many different servers and may be in the control of different parties along the way, often with unknown security levels.[90] Cloud users' information may be disclosed to third parties for advertising purposes, accessed by government agencies, or even viewed by CSP administrators or help desk operators.[91] Once information is uploaded to the cloud, it becomes very difficult, if not impossible, to control, track, or delete.[92] Much of this information is in the hands of private parties. This does not, however, put it out of the

---

87. *About Legislation, Security and the Patriot Act*, CLOUDME, https://www.cloudme.com/en/legal/patriotact (last visited Oct. 25, 2014).

88. Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. TECH. L. & POL'Y 229, 235-38 (2011).

89. JANSEN & GRANCE, *supra* note 70, at 30 (maintaining that for security in the cloud, "[d]ata must be secured while at rest, in transit, and in use, and access to the data must be controlled").

90. Bender, *supra* note 65, at 489.

91. *See* Gervais & Hyndman, *supra* note 22, at 77-78 ("As a technical matter, providers of Cloud services can probably access any material uploaded to the Cloud."); *see also* Rauhofer & Bowden, *supra* note 26, at 11-12 (discussing access by third parties to EU personal data).

92. Gervais & Hyndman, *supra* note 22.

reach of governments. As provided in one report to the European Parliament, "[T]he root problem is that cloud computing breaks the forty year old legal model for international data transfers . . . . [Once] data is transferred into a cloud, sovereignty is surrendered."[93] The lack of transparency of many cloud services and limited ability to audit services increase the apprehension of users and mitigate their ability to control risks.[94] As a result, the cloud may be essentially "off-limits" for certain users, particularly those in healthcare or financial industries.[95]

Security risks associated with the shared cloud infrastructure are far from hypothetical.[96] Major CSPs have reported problems with their services including security breaches and loss of customer data. Malfunctions may result from software or hardware failures or even outside attacks on the cloud structure. The larger the cloud structure becomes, the greater the "attack surface" for those intending to cause damage (such as hackers) have available for exposing operating errors and finding weaknesses.[97] Hackers posing as customers may also use their access to the cloud to exploit vulnerabilities in the structure.[98] Storage of data by many parties may result in breakdowns of data management such as virtualization "sprawl," commingling of data, or data leaks.[99] For example, the discount IaaS storage provider

---

93. Bigo et al., *supra* note 65, at 35.

94. W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 79, 112 (2012); *see* Gasser, *supra* note 50, at 16 ("[The] debate in the EU is illustrative in this respect, where the lack of transparency in contracts about responsibilities and privacy-relevant practices has been identified among the factors that might further increase privacy vulnerabilities for consumers of cloud services.").

95. Jonathan J.M. Seddona & Wendy L. Currieb, *Cloud Computing and Trans-Border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance*, 2 HEALTH POL'Y & TECH. 229, 237-40 (2013) ("[A]ny health-care organizations using an external IT provider must now ascertain whether all sub-contracted parties meet regulatory rules."). Further, "[a]s a precondition for entering into a cloud computing agreement, the controller is expected to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the potential risks and benefits from a data protection perspective." *Id.* at 237.

96. *See, e.g.*, Carmeli, *supra* note 62, at 7. In 2011, a failure in Dropbox's code allowed any of its twenty-five million user accounts to be accessed with any password.

97. Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 436 (2013).

98. *See* Nancy J. King & V.T. Raja, *Protecting the Privacy and Security of Sensitive Customer Data in the Cloud*, 28 COMP. L. & SEC. REV. 308, 309 (2012); David Krebs, *Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union*, 10 CAN. J.L. & TECH. 29, 34-35 (2012).

99. King & Raja, *supra* note 97, at 436 ("VM sprawl describes a situation where too many VMs are provisioned, making the management of the VMs more complex. When this occurs and the CSPs' data tracking and documentation practices are inadequate, it may be impossible to identify data at a specific point in time.").

Digitalocean had a software malfunction with the potential to be damaging to its former customers. The software that Digitalocean used to manage its servers was not erasing the data of its customers after they stopped using the service.[100] Data that should have been deleted by Digitalocean leaked into other accounts and was viewable by other Digitalocean customers.[101]

In addition to technical or security-related problems, the illegal acts of some users sharing the infrastructure may have negative impacts for the security and access of all users. In the well-publicized case of the storage provider Megaupload, the company's servers were seized as a result of large-scale copyright infringement taking place using its server infrastructure. As a result, many users were left without access to the service or their data.[102] Many users lost data including business information and even family photographs that had nothing to do with the criminal activity of some Megaupload users.[103] Megaupload users have few remedies available to compensate for the lost data.[104]

Unclear or unfavorable terms for removing data provide another form of risk for users.[105] To take a recent example, a well-funded CSP called "Nirvanix," which was poised to become a competitor to AWS and Google, apparently ran into monetary problems.[106] Nirvanix provided its users with only two weeks to obtain their data before filing for bankruptcy on October 1, 2013, just after the period expired.[107] Even for computer savvy users of cloud computing, two weeks provides very little

---

100. Robert McMillan, *Cloud Computing Snafu Shares Private Data Between Users*, WIRED (Apr. 2, 2013, 4:50 PM), http://www.wired.com/wiredenterprise/2013/04/digitalocean/.

101. *Id.* at 1; *see also* Bender, *supra* note 65, at 488-89.

102. Pham, *supra* note 10, at 168.

103. Bryan E. Arsham, *Monetizing Infringement: A New Legal Regime for Hosts of User-Generated Content*, 101 GEO. L.J. 775, 785 (2013); Benton Martin & Jeremiah Newhall, *Criminal Copyright Enforcement Against Filesharing Services*, 15 N.C. J.L. & TECH. 101, 147-49 (2013).

104. Anjanette H. Raymond, *Heavyweight Bots in the Clouds: The Wrong Incentives and Poorly Crafted Balances That Lead to the Blocking of Information Online*, 11 NW. J. TECH. & INTELL. PROP. 473, 496-97 (2013) ("[N]o law in the E.U. or U.S. provides protections when an *entire* website is blocked.").

105. In the EU, an expert group has been formed and is focusing on problems with cloud computing contracts in the areas of pre-contractual information, data portability upon switching services, liability for non-compliance with data protection obligations, data location and security, and modifications of cloud computing contracts. *Topics To Be Covered by the Expert Group*, EUR. COMMISSION (Oct. 5, 2014, 10:17 PM), http://ec.europa.eu/justice/contract/files/expert_groups/25112013_discussion_paper_en.pdf.

106. David Streitfeld, *Even Early Adopters See Major Flaws in the Cloud*, N.Y. TIMES (June 11, 2014), http://bits.blogs.nytimes.com/2014/06/11/even-early-adopters-see-major-flaws-in-the-cloud/.

107. *Id.*

time to remove data and find a new service. In the case of an unsophisticated SME or consumer, the feat is even more difficult. A term of this type is not unusual. Many CSPs provide very short timetables, or vague schedules for removing data (i.e., "commercially reasonable"). Depending on the needs of the user (size and format of the data) a time period of even six months to make the transition may be a challenge. The requirement that the change take place in a shorter period, thirty to sixty days, may be commercially impossible.[108] Assuming the transfer must take place over a network (as opposed to a disk transfer), a large amount of data could take weeks to transfer.[109]

More general cloud risks include limited availability of data, loss of data portability, and jurisdictional exposure.[110] In addition, there are more individualized risks that will impact different cloud consumers, depending on their use of the service, national compliance requirements, or sector-specific regulations including fines for noncompliance. For some users, there may be significant costs associated with data breach notification requirements if customer data stored in the cloud is lost or exposed.[111] Other cloud consumers will have specialized risk considerations regarding document and preservation requirements for discovery. There may even be a loss of constitutional protections in the case of permissive contract terms.[112] Contracts that allow for disclosure and sharing of data may even have implications for a cloud consumer asserting that documents stored on the cloud are private.[113]

---

108. MILLARD, *supra* note 17, at 52. QMUL found a wide range from immediate deletion to six months. Many providers allowed fifteen to thirty days, but potentially less time if the AUP was breached.

109. Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, 53 COMM. ASS'N COMPUTING MACH. 50, 56 (2010) ("[A]ssume that we want to ship 10 TB from U.C. Berkeley to Amazon in Seattle, Washington. Garfinkel measured bandwidth to S3 from three sites and found an average write bandwidth of 5 to 18 Mbits/second. [19] Suppose we get 20 Mbit/sec over a WAN link. It would take 10 ∗ 1012 Bytes / (20 × 106 bits/second) = (8 × 1013)/(2 × 107) seconds = 4,000,000 seconds, which is more than 45 days. Amazon would also charge you $1000 in network transfer fees when it received the data.").

110. Gabriela Zanfir, *The Right to Data Portability in the Context of the EU Data Protection Reform*, 2 INT'L DATA PRIVACY L. 149, 158-61 (2012); Matthew B. Becker, *Interoperability Case Study Cloud Computing* 20 (Harvard Univ., Berkman Ctr. for Internet & Soc'y Research Publ'n Working Paper No. 2012-5, 2012), *available at* http://www.ssrn.com/abstract=2031109.

111. King & Raja, *supra* note 98, at 314-15. This is currently the case in the United States and has been proposed in the EU.

112. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010). The court provided, "[A] subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . ." *Id.*; *see also* Jay P. Kesan, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 416-17 (2013).

113. Kesan, *supra* note 112.

III. EU REGULATORY FOCUS ON CONTRACT TERMS AND CONDITIONS

The following Part provides an overview of EU DPL and considers how the rules interact or interface with contracting practices commonly used in cloud computing. Specifically, what are the requirements placed on users of cloud services and what obligations do CSPs have when outsourcing aspects of their services to third parties pursuant to EU DPL? Although many of the observations made in this Part apply to cloud computing in general, I place particular focus on legal problems present in public cloud models. In particular, I consider conflicts between common cloud computing contract arrangements and EU DPL.

The intersection of EU DPL and contracts illustrates the friction between national laws and contract terms for two reasons. First, conflicts between EU DPL and common cloud computing practices are relatively apparent.[114] Second, in an area where case law is sparse, and guidance is often limited to authoritative (although not binding) sources, contracts have been given a particularly prominent role.[115] Finally, this Part evaluates whether greater state-sponsored regulation, EU or otherwise, is desirable. In making this determination, I consider whether nation states ought to become more involved in what is happening on the cloud.

Privacy is an amorphous concept that has been notoriously difficult to define.[116] Data privacy, as covered in the EU Data Protection Directive 95/46/EC, is derived from a broader concept of the right to privacy, which is recognized as a fundamental human right in the EU.[117] Based on that foundation, EU DPL only allows the processing of personal data under specific and limited circumstances.[118] The focus and policy behind EU DPL is based on the data privacy rights of the "data subject" or the

---

114. *See, e.g.*, Council Directive 95/46/EC, art. 7, 1995 O.J. (L 281) 31.

115. These authoritative nonbinding sources are primarily from EU regulators, often Data Protection Authorities (DPAs). *See, e.g.*, *Guidance on the Use of Cloud Computing*, INFO. COMMISSIONER'S OFFICE, http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing (last visited Oct. 17, 2014). Although case law remains limited, at least two important decisions were reached in 2014: in the EU, Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (May 13, 2014), and in the United States, *American Broadcasting Co. v. Aereo, Inc.*, 134 S. Ct. 2498 (2014).

116. LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC, AND LIMITS 4 (2002).

117. LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 82-98 (2014); *see also* Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, June 1, 2010, 4.XI.1950, *available at* http://conventions.coe.int/treaty/en/treaties/html/005.htm. For U.S. constitutional privacy protections, see Fred H. Cate & Beth E. Cate, *The Supreme Court and Information Privacy*, 2 INT'L DATA PRIVACY L. 255, 256-58 (2012).

118. Council Directive 95/46/EC, art. 7, 1995 O.J. (L 281) 31, 40.

"identified or identifiable natural person" the data concerns.[119] The basic EU DPL framework is provided in Directive 95/46/EC (Data Protection Directive) and Directive 2002/58/EC (E-Privacy Directive).[120] In this Part, I focus on the former.

The Data Protection Directive applies to all processing of data that is deemed personal.[121] The term "personal data" is broadly construed, applying to "any information relating to an identified or identifiable natural person."[122] If personal data is made truly anonymous, and the data subject cannot be identified, the data is no longer considered "personal data."[123] However, the standard for showing that data is sufficiently anonymous is an arduous one and is not satisfied even with encryption in most cases.[124] In addition to processing restrictions, EU DPL limits transfers of personal data to countries without adequate levels of protection.[125] These aspects of EU DPL are particularly burdensome for cloud computing.

EU DPL places heavy burdens on the actor in control of the personal data and substantial limits on the use and reuse of information. In addition to requiring that the processing involved is for "legitimate purposes," the data must be appropriately protected, not retained longer than necessary, accurate, and observe other rights of the individual to whom the data concerns.[126] Under the EU directive, the term "processing" includes almost any collection or use of personal data, including uploading personal data to the cloud.[127] Although the Data Protection Directive does not provide an absolute right to privacy or limit to the processing of personal data altogether, the protections it provides to the data subject are expansive.[128]

---

119. *Id.* art. 2.

120. Council Directive 2002/58/EC, 2002 O.J. (L 201) 37-47.

121. Directive 95/46/EC, *supra* note 118, art. 2(a)-(b).

122. *Id.* art. 2(b); *see also Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 15.

123. Council Directive 2002/58/EC, *supra* note 120, recital 26.

124. Millard, *supra* note 17, at 176-77; Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, at 29 (Apr. 10, 2014) [hereinafter WP 216], *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf ("State-of-the-art encryption can ensure that data is processed to a higher degree, . . . but it does not necessarily result in anonymisation."); *see also* Council Directive 95/46/EC, *supra* note 118, recital 26.

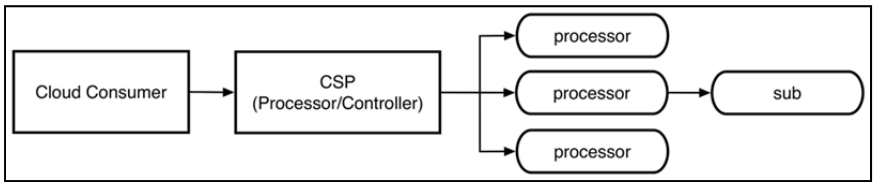
125. Council Directive 95/46/EC, *supra* note 118, art. 25.

126. *Id.* art. 6.

127. Lanois, *supra* note 15, at 24.

128. Council Directive 95/46/EC, *supra* note 118, art. 13.

EU DPL identifies the central parties in data protection law as "controller," "processor," "third party," and "data subject."[129] Pursuant to EU DPL, "controllers" and "processors" accessing data are treated differently.[130] Data controllers have the ultimate responsibility for treating the personal data entrusted to them in conformance with EU DPL.[131] Processors work "on behalf of" or "under the instruction of" data controllers.[132] Processors also have more limited liability under the DPL regime, on the condition that they only operate in that narrow capacity—under the instructions of the controller.[133] The processor's reduced liability and limited duty to the data subject entail protecting the confidentiality of personal data and maintaining an adequate security level, among other duties.[134]



In the above graphic, the cloud consumer is the controller (and possibly also the data subject). Here the cloud consumer transfers data to the CSP provider, who will likely be a processor, but may also be a controller (or subcontroller) depending on its use of the data. Finally, the CSP processor (or controller) transfers data throughout their supply chain to subcontractor processors (infrastructure providers, etc.) that may further transfer data to subprocessors.

Although the controller may enter into the contract, the data subject retains certain rights over their data.[135] These rights are both general and

---

129. *Id.* art. 2; *see also* Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor," 00264/10/EN/WP 169, at 17-18 (Feb. 16, 2010) [hereinafter WP29 169], *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

130. Council Directive 95/46/EC, *supra* note 118, art. 17(2)-(3). Processors must act only on the instructions of controllers. WP29 169, *supra* note 129; *see also* EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 51-53 (2013) (describing processor controller relationship).

131. Council Directive 95/46/EC, *supra* note 118, art. 2(d); Szilvia Varadi et al., *The Necessity of Legally Compliant Data Management in European Cloud Architectures*, 28 COMP. L. & SEC. REV. 577, 579 (2012).

132. Council Directive 95/46/EC, *supra* note 118, art. 2(e).

133. *Id.* art. 17(3).

134. Hustinx, *supra* note 30, ¶ 31; MILLARD, *supra* note 17, at 193-219.

135. Lee A. Bygrave, *Transatlantic Tensions on Data Privacy* (Transworld Working Paper 19, 2013), *available at* http://www.transworld-fp7.eu/wp-content/uploads/2013/04/TW_WP_19.pdf (maintaining that the data subject is "largely prevented from disposing of their statutorily

specific, including the right to access data, correct incomplete or incorrect information, and require erasure.[136] A cloud consumer moving data to the cloud must make certain the rights of the data subject are considered. This requires assessing the cloud structure for the ability to comply with these obligations.

In the EU, regulators are concerned that cloud computing technology has the potential to diminish or dilute the level of control cloud consumers have over their data.[137] EU regulators are considering the impact that cloud contract terms may have on cloud consumers.[138] A demanding data protection regime, coupled with expansive consumer protection regulations, requires that CSPs alter some common contracting practices and contract terms to meet EU compliance requirements.[139] At present, many widespread cloud computing practices conflict with EU regulations.[140] Compliance with EU laws may require that CSPs adjust their business models. Specifically, the data protection regime in the EU requires that CSPs limit their use of data in ways that may not be required in other jurisdictions.

A. Applying EU DPL to Cloud Computing

In the cloud computing scenario, the user of the service (cloud consumer) will be the data controller in most circumstances.[141] As a controller, the cloud consumer retains the greatest level of responsibility. By way of example, an SME, municipality, or a multinational corporation placing customer or user data in the cloud would be considered a controller. The CSP providing the service would be the processor. A CSP acting solely as a means of transit or providing infrastructure will remain a processor. However, if the CSP processor utilizes the data in a manner that goes beyond processing or for their own purposes (e.g., repurposing data for behavioral advertising, data mining, or certain value added services) the CSP may also be considered a

---

enumerated rights over use of the data, at their discretion or according to the dictates of the market").

136. Council Directive 95/46/EC, *supra* note 118, art. 12; *see also id.* art. 6(1).

137. Bigo et al., *supra* note 65.

138. *See, e.g.*, *Topics To Be Covered by the Expert Group*, *supra* note 105.

139. Samson Yoseph Esayas, *A Walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data*, 28 COMP. L. & SEC. REV. 662, 664-68 (2012); Michael L. Rustad & Maria Vittoria Onufrio, *Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy*, 14 J. BUS. L. 1085, 1116 (2014) ("The ubiquity of one-sided TOUs for the U.S. consumer market is undisputed; however, these agreements are not enforceable in Europe.").

140. Anthony Gray, *Conflict of Laws and the Cloud*, 29 COMP. L. & SEC. REV. 58 (2013).

141. Krebs, *supra* note 98, at 62-63.

controller or joint-controller.[142] As a controller, the CSP is subject to a greater duty of care and liability to the data subject. Despite designations in contractual terms, the EU DPL will apply to the CSP acting as controller because the responsibility cannot be abrogated or avoided by contract.[143] Stated differently, EU DPL "creates immutable defaults," which cannot be changed by agreements made between private parties.[144] Therefore, contract terms providing that the CSP will always be considered a processor are not effective.

Although contract terms cannot be used to change the factual controller/processor designation, contracts are used as a means to ensure or enhance the rights of data subjects. One explicit contractual requirement is article 17 of the Data Protection Directive, requiring that controllers take "appropriate technical and organizational measures to protect personal data."[145] Additionally, article 17 requires that "[t]he carrying out of processing by way of a processor must be governed *by a contract* or legal act binding the processor to the controller."[146] Further, article 17 requires that the "the processor shall act only on instructions from the controller."[147] Based on the directive, the cloud consumer (data controller) entering into a contract with a CSP (data processor) must enter into a contract that allows for a certain level of control over the CSP. The instructions the controller places on the data must be followed throughout the chain of contractors.

In the case of public cloud services, the structure of the services often makes it difficult for cloud consumers to obtain a contract that meets the requirements of article 17. Cloud consumers generally retain very little, if any, control over the acts of the CSPs and their subcontractors—particularly in a large public cloud setting.[148] Uploading information onto an unknown cloud computing system with little control over data transfers does not comply with this requirement. In the case of traditional IT outsourcing, where contracts "flowed in the same direction," compliance with article 17 was potentially easier. Article 17 is in many

---

142. Hustinx, *supra* note 30, ¶ 31; *see also* Article 29 Data Protection Working Party, Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 01935/06/EN WP 128, at 10-11 (Nov. 22, 2006), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf [hereinafter WP 216].

143. *Id.*

144. Schwartz, *supra* note 75, at 1658.

145. Council Directive 95/46/EC, *supra* note 118, art. 17(1).

146. *Id.* art. 17(3); *see also id.* art. 28(3) (providing data protection authorities with the abilities to police CSPs (and others) compliance with article 17).

147. *Id.* art. 17.

148. FORGÓ ET AL., *supra* note 77, at 26-27.

ways ill-suited for the complex contracting practices in cloud computing. Although EU DPL requires that "the processor shall act only on instructions from the controller," the notion that the cloud consumer/data controller has the power to instruct a CSP/processor such as Google or Amazon on how data is processed is out of touch with the reality of most cloud computing services.[149]

The current EU DPL envisions a much more limited contractual network than exists in typical public cloud services.[150] Contractual solutions that have filled this gap in other areas, such as the present European Commission (EC) standard contractual clauses (SCCs), are often considered inadequate to meet EU DPL requirements in the cloud.[151] The terms set forth in SCCs are rigid, are modeled after more traditional data transfers, and require the approval of national DPAs, adding time and expense. Moreover, SCCs must be adopted as is and do not allow for changes to meet the needs of the cloud service.[152] This inflexibility is often a poor fit for a user attempting to contract onto a preexisting structure. Similarly, binding corporate rules (BCRs), which are an option for large multinational firms processing data, have been proven inadequate for CSPs using a diverse set of actors focused on rapid expansion.[153] Further, getting BCRs approved is both time consuming and expensive, which is a poor match for the cloud model.[154]

Regulators, cloud consumers, and CSPs have many questions on the way EU DPL applies to cloud computing and opinions on how it ought to apply. How much notice is the CSP required to provide the controller regarding its processing activities? Must CSPs ensure that all the terms in the contract with a cloud consumer are reflected in agreements with subcontractors? Should more liability be placed on processors, particularly in arrangements where controllers have very limited ability

149. Blume, *supra* note 78, at 142.

150. *Id.* at 141.

151. FORGÓ ET AL., *supra* note 77, at 9; *see* Council Directive 95/46/EC, *supra* note 118, art. 26(2); *see also* Commission Decision 2001/497/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Council Directive 95/46/EC, 2001 O.J. (L 181/19); Commission Decision 2004/915 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385/74).

152. Ninja Marnau & Eva Schlehahn, *Tclouds D1.2.2 Cloud Computing: Legal Analysis*, TCLOUDS 66 (Oct. 3, 2012), http://www.tclouds-project.eu/downloads/deliverables/TC-D1.2.2_Cloud_Computing-Legal_Analysis_M12.pdf (finding that SCCs become difficult to use once several layers of customers and subcontractors become involved as they require that the parties conclude a multitude of agreements).

153. Seddona & Currieb, *supra* note 95, at 229, 239.

154. Marnau & Schlehahn, *supra* note 152, at 79.

to negotiate terms and control very little of the cloud infrastructure? In the next Subpart, I evaluate the EU approach to some of these queries.

B. Conflicts Between Contracting Structure and EU DPL

It may be difficult for CSPs to employ adequate controls to ensure that all partners or subcontractors are handling the personal data of EU citizens in a lawful manner. The structure of the cloud service is essentially undetectable to the cloud consumer and the contracts generally provide the user with very little control over their data once it enters the cloud service.[155] Contracts provide very few limits on data usage and rarely contain a right to audit the service for compliance. For these reasons, it becomes difficult for the cloud consumer to assess the parties in the service chain or appreciate the data protection risks a service may involve.

The challenge of adopting cloud computing in a manner that is consistent with current EU legislation has received a great deal of attention. In particular, the EC, European Data Protection Supervisor, and the article 29 Working Party (WP29) released opinions on cloud computing (WP196).[156] The opinions and reports focus on unlawful contract terms as a major impediment to wider use of cloud computing in Europe.[157] Currently, the contract terms offered by many CSPs fail to meet EU legal requirements, particularly in the area of data protection law, but also consumer protection regulations.[158] In the following Subpart, I consider the foremost contract compliance issues considered in opinions issued by EU authorities.

The central issue considered in the WP29 cloud computing opinion is whether cloud computing services are compliant with EU data protection law. Among other concerns, the WP29 points out the risks that the diffuse structure of cloud services presents. A major theme of the WP29 is the lack of transparency and clear chain of accountability in cloud services.[159] The WP29 succinctly summarized the organization of the cloud and the resulting legal requirements as follows:

---

155. Yann Padova, *What the European Draft Regulation on Personal Data Is Going To Change for Companies*, 4 INT'L DATA PRIVACY L. 39, 45 (2014).

156. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30.

157. *See, e.g.*, Hustinx, *supra* note 30, ¶¶ 1, 5.

158. FORGÓ ET AL., *supra* note 77, at 9-10.

159. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 6, 8.

> Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC.[160]

Despite the position of the WP29, the cloud consumer is generally not apprised of the structure, changes in the parties operating the service, or even supplied with a guarantee that the terms in the original agreement will be imposed on all subcontractors.[161] The WP29 is not alone in arguing that the current system of contracting may not be in accord with EU requirements.[162] In the "unleashing the cloud" paper published by the EC, a section titled "problems with contracts" focuses on confusion or uncertainty in contract terms on issues such as liability for service failures, compensation for losses, and the uncertainty of user rights as areas of concern in cloud computing.[163]

In a response to the EC's "unleashing the cloud" opinion, the European Data Protection Supervisor focused on the current "contractual asymmetry" that exists between CSPs and cloud consumers.[164] The European Data Protection Supervisor provided that compliance with EU data protection law for data controllers is "very difficult or even impossible" in a cloud computing environment.[165] Adding to the asymmetry is the wide variation of operational practices among CSPs. Operational decisions like data storage, deletion policies, data location, and transfer of data to third parties are not standardized and may vary considerably depending on the provider. Recognizing that outsourcing important aspects of infrastructure to subcontractors may conflict with EU data protection law, the WP29 provides some guidance on the matter.

> In the view of the WP29, the processor can subcontract its activities *only on the basis of the consent* of the controller, which may be generally

160. *Id.* at 9.

161. Robinson et al., *supra* note 66; FORGÓ ET AL., *supra* note 77, at 16-17 (discussing French DPA approach that "contractual obligations stipulated in the original service contract should be passed on to the sub-processor").

162. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30.

163. Eur. Comm'n, *Unleashing the Potential of Cloud Computing in Europe*, EUR-LEX 5 (Sept. 27, 2012), http://eurlex.europa.eu/LexUriServ.do?uri=COM%3A2012%3A0529%3AFIN%3AEN%3APDF.

164. Hustinx, *supra* note 30, ¶ 1.

165. *Id.* at 6.

> given at the beginning of the service with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract.[166]

The WP29 also provides that there "should be a clear obligation" of the CSP to name all the subcontractors commissioned in order to create conforming contracts.[167] In addition, given the current structure of many cloud services, the WP29 notes the risk of data being used illegally by subcontractors for further processing.[168] Further, the terms agreed to in the contract between the cloud consumer controller and the CSP processer should also be imposed throughout the chain of subcontractors.

In its evaluation, the WP29 does not tailor its interpretation of EU DPL to fit the dynamic structure of cloud computing services and the economics of the cloud storage market. As is stated throughout the WP29 opinion, the structure of the cloud and the partners added may change dramatically during the life of the service.[169] The WP29 acknowledges this circumstance, but does not create a "cloud computing exception." The notice and consent requirements for adding subcontractors, and the requirement that the controller retains control throughout the service, remain.[170] Although the requirements are designed with traditional IT outsourcing arrangements in mind (contracts "flowing" in one direction), they apply to the cloud model. Requiring prior notice and consent seems unworkable under many existing cloud models.[171] The structure of the cloud service, and many of the contracts,

---

166. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 10.

167. *Id.* Guidance also exists at the national level. For example, Spanish data protection law has detailed requirements mandating notice of the use of subcontractors, with some exceptions. Specifically, article 21 of the Spanish Data Protection Law provides, "The data processor may not subcontract to a third party any processing commissioned to him by the data controller, unless he has received authorization to do so." *See* Royal Decree 1720/2007, of 21 December, Which Approves the Regulation Implementing Organic Law 15/199, of 13 December, on the Protection of Personal Data art. 21 (B.O.E. 2008, 979) (Spain), http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/reglamentolopd_en.pdf.

168. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*, *supra* note 30, at 11.

169. *Id.* at 5.

170. *Id.* at 9.

171. National regulators have taken different views regarding the compliance of individual cloud services. For example, the Swedish DPA, considering contracts of several providers to be used by municipalities, found in particular that Google's contract terms allowing Google to transfer data widely to subcontractors outside of Google's corporate structure did not meet the requirements of Swedish data protection law. Dan Svantesson, *Data Protection in Cloud Computing—The Swedish Perspective*, 28 COMP. L. & SEC. REV. 4, 7 (2012). However, the Norwegian DPA also reviewed the use of Google Applications by a municipality and determined

is already in place making prior notice difficult. I do not contend that notice should be ignored. However, a system of notice that better fits the cloud model would have more achievable results.

The question regulators are wrestling with is which method or model is most likely to be effective in allowing cloud computing to grow while also obtaining compliance from CSPs. In the EU, a focus on wider, lawful deployment of cloud computing has concentrated on contract terms and conditions. Rather than looking solely at a legislative solution, the EC is embracing private law methods of regulation and has specifically focused on creating "safe and fair contract terms and conditions" as a core principle.[172] EU regulators are pushing a more "complete" contract that will afford users more meaningful terms by providing information about the parties to the service, the roles and terms between them, and the specific guarantees of each party.[173] This would require making some changes in the way cloud computing contracts are currently deployed. For example, eliminating terms that allow CSPs to make unilateral contract changes without consent is a starting point. A further change might be to require that jurisdictional and dispute resolution terms, particularly in choice of forum, are in accord with EU law.

The EC's focus on evaluating contract terms to determine their lawfulness under EU DPL is an important step. Contracts have the potential to enhance data privacy in cloud computing as well as increase compliance with other EU legal requirements. Most notably, contracts provide the cloud consumer with specific information regarding permissive and prohibited uses of cloud consumer data by the CSP. A set of "model" or standard terms may also serve as a guide to cloud consumers by providing a warning against the use of cloud services that depart from the model terms provided by the EC. For CSPs, clearer terms or regulations may provide a clearer path to delivering compliant clouds in the EU.

Model contract terms may prove more advantageous than creating new laws and regulations that are difficult to enforce. However, assuming the usefulness of such terms makes presumptions that may be unwarranted. First, it requires that terms be read and understood. As

---

that the contract was compliant with Norwegian Law. Norwegian Data Protection Authority (Datatilsynet), *New E-Mail Solution for the Municipality of Narvik—Google Apps*, NORWEGIAN DATA PROTECTION AUTHORITY (Sept. 21, 2012), https://www.datatilsynet.no/Global/english/12%200699%20Datatilsynet-Narvik%20kommune-en.pdf.

172. Eur. Comm'n, *supra* note 163, at 11-13.

173. *Id.* at 10.

with other standard click-wrap terms, almost all evidence suggests that this is not happening.[174] Second, the usefulness of the terms essentially requires that the providers are willing to adopt and comply with the terms. In the current market, the argument has been that highly regulated terms will destroy many of the advantages of cloud computing, particularly in the public cloud model.[175]

C. Proposed Regulation: Changing the Balance of the Contract?

Putting more responsibility on CSP processors might also reduce the current risk/liability imbalance that exists in many cloud computing agreements. CSPs often disclaim all liability for their services and put the burden of complying with regulatory requirements on cloud consumers.[176] One author described the role of CSPs regarding their users' compliance requirements as "ill-defined, misunderstood, or poorly accommodated by providers."[177]

The current controller/processor separation in data protection law allows for this apportionment of risk in the contract. Creating additional and independent processor responsibilities might help to reduce this disproportion.[178]

In many cases, the liability assumed by the parties does not reflect the level of control they have over cloud service. Although it is the cloud consumer (or controller) that decides to use the service, the CSP (or data processor) often has a much greater ability to mitigate cloud risks. Current proposals for data protection reform in the EU may help to bring more balance to this relationship.[179] Requiring processors to take on additional responsibility, particularly in areas where they have the most control, could result in a higher level of protection for cloud consumers. For example, article 26 of the proposed data protection regulation builds on article 17 of the Data Protection Directive and takes steps in shifting

---

174. Hayes, *supra* note 112, at 510-12.

175. *E.g.* Millard, *supra* note 17, at 47, 52 (discussing IBM terms and conditions making some allowances for different jurisdictions).

176. *Id.* at 59. This study found that the "vast majority" of CSPs disclaimed liability in their standard contracts. However, the study also noted that from 2010 to 2013 contract terms were much more tailored to the cloud consumers' home jurisdictions (instead of providing the broad U.S.-style disclaimers for all users).

177. *Id.* at 85.

178. Blume, *supra* note 78, at 144-45.

179. Bygrave, *supra* note 117, at 71-75 (providing an overview of current EU DPL reform process). Pursuant to EU law, a directive requires harmonization of legislation by the member states independently while a regulation creates standards implemented uniformly across the EU. *See, e.g.*, Schwartz, *supra* note 75, at 1642.

additional requirements to the processor in certain situations, including providing notice. The proposed regulation would require the following:

> 2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall . . .
> (d) enlist another processor only with the prior permission of the controller[180]

If the cloud consumer controller is provided with notice of all subcontractors (acting as sub- or sub-subprocessors) in the contract, it may help the controller to identify the layers of the cloud computing service. Further, the proposed regulation states, "If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24."[181] Although the processor is not made an equal to the controller in the proposed regulation, processors will have expanded obligations if they go beyond general processing.[182]

These proposed requirements acknowledge the situation present in many cloud computing scenarios. The controller cloud consumer often has very limited control over the processing. The data processor CSP is in a much better position to prevent data loss or other harms related to unlawful processing by subcontractors or other third parties with access to the cloud consumers' data.[183] By requiring that cloud consumers are informed of the structure of the cloud computing service as well as increasing processor liability for breaches, CSPs might also pay more attention to the compliance requirements of their users.[184]

EU data protection authorities have offered guidance nationally on the use of cloud services. Often, the advice follows the A29 party

---

180. Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) at 58, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

181. *Id.* at 11, general obligations § 1, art. 26(4); *see id.* at 10 (articles 28 and 30, specifically 30, which requires processors to keep data secure).

182. Bygrave, *supra* note 117, at 73-74 (outlining increased processor responsibilities).

183. Padova, *supra* note 155, at 45-46 (discussing additional requirements placed on subcontractors).

184. *Id.* at 51-52 (discussing increased fines and liability).

opinion in addition to any local compliance requirements.[185] In the UK, one data protection authority suggested the following:

> The controller should be able to avail of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. This could be arranged by ensuring that the processor is directly liable toward the controller for any breaches caused by any sub-processors he has enlisted, or through the creation of third party beneficiary right for the benefit of the controller in the contracts signed between the processor and the sub-processors or by the fact that those contracts will be signed on behalf of the data controller, making this later a party to the contract.[186]

This would appear to go even further than the requirements suggested by the WP29. In the situation suggested here, the controller would maintain direct privity of contract with the providers and subcontractors, thus maintaining clear avenues for recourse.[187] Although it seems unlikely that many CSPs would entertain such an arrangement, it would increase the controller's connection to all parties in the contracting chain.

When considering the possibility of rearranging processor liability, arguments that the controller remains liable should not be completely discounted. The controller cloud consumer often remains in the best place to prevent harm. After all, it is the cloud consumer that decides to use the service and determines if the service is appropriate for the type of data that will be stored with the CSP. However, given the imbalance in the bargaining relationship and the lack of information regarding the many layers of cloud computing services, placing the balance of liability on the cloud consumer has negative consequences for trust in the cloud, and ultimately the uptake and use of the services. A more balanced approach, including an agreement that places clear duties on the processor, might better apportion the risk. This is particularly true in large public cloud models.

IV. CONCLUSION

If the cloud service operates correctly, the cloud consumer is unlikely to be aware of the complex structure that their data traverses. Cloud services claim to make users more efficient with products that are

185. *See, e.g.*, *Cloud Computing: A Guide for Data Controllers*, OFFICE DATA PROTECTION COMMMISSIONER 6 (July 1, 2012), http://www.dataprotection.gov.je/NR/rdonlyres/C24B19CD-4124-430E-B644-723058016DC8/0/20120912CloudComputingAGuideforDataControllers.pdf.

186. *Id.*

187. Cafaggi, *supra* note 52, at 568-69.

"automatic and effortless."[188] In many cases, the services deliver much of what their advertising promises—an inexpensive bridge to state of the art computing and data storage. However, if bumps are encountered along the way, the cloud consumers may have considerable difficulty recovering information or even finding a party to hold liable. Many of the protections cloud consumers are dependent upon are governed largely by the terms of their contract, which is generally more favorable to the CSP. European cloud consumers, including SMEs and municipalities, may find it particularly difficult to meet their compliance requirements, particularly when contracting on standard terms.

Although the flexible cloud structure may be economically efficient, allocation of responsibility and control over the various actors in the chain becomes less clear. In addition to possible diluted accountability, the various providers making up this chain impact other issues like security, compliance with national laws, and trust in the services.[189] Lack of trust in cloud computing services remains a major impediment to the uptake of the technology on a wider basis. Even if flexibility is an important asset, the current structure of contracts contains aspects that are largely unfair to cloud consumers. As a result, many users, particularly those in highly regulated sectors, have been almost categorically excluded from cloud computing. These potential cloud consumers have some of the greatest potential as new users and may also be some of the largest beneficiaries of the economy of scale offered by cloud computing. Although "Balkanization" of the cloud is not generally seen as a positive step in cloud computing development, limiting some services to subcontractors in certain geographic regions may become the only solution for some users.[190]

In the case of computer technology, rapid changes and complex business models have received great deference from regulators who

---

188. *Apple—iCloud*, INTERNET ARCHIVE, http://web.archive.org/web/20111010040417/https://www.apple.com/icloud/? (last visited Nov. 7, 2014) (providing an archived screenshot of website as it displayed on October 10, 2011); *see also* iCloud, APPLE, http://www.apple.com/icloud/ (last visited Nov. 3, 2014) ("iCloud does it all automatically.").

189. Daniele Catteddu, *Security & Resilience in Governmental Clouds—Making an Informed Decision*, EUR. NETWORK & INFO. SEC. AGENCY (ENISA) 29-30 (2011), http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

190. The term "balkanization" as used in this Article means the break-up of global cloud computing services, along national or regional lines, based on apprehension or fear or storage in foreign jurisdictions. Balkanization has the potential to limit the economic benefits that cloud computing provides when deployed globally. Simon Bradshaw et al., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, 19 INT'L J.L. & INFO. TECH. 187, 192 n.14 (2011).

adopt a "restrained approach" to regulating technology beyond the parties' contract.[191] Following this trend of restrained regulation, the impact of the rules set by parties in a cloud computing contract have even greater effect than contract terms do in other more highly regulated industries—particularly in areas where local regulation is more easily enforceable. The "restrained approach" to Internet or technology regulation often seen in the United States may not hold in the EU.[192] Nevertheless, greater regulation is probably needed in this area on both sides of the Atlantic.

By making the cloud more predictable, secure, and fair for cloud consumers on a contractual basis, some of those currently excluded may be able to start using the cloud. A first step in this process is providing clearer contract terms and standards that will allow users to understand the structure of services and to determine if the partners to the service meet compliance requirements.[193] The EU requirement stated by the WP29, that a contract or other agreement be in place and that the cloud consumer be informed of subcontractors, are steps worth replicating in other jurisdictions. Placing greater statutory liability requirements on CSP processors for losses within their control is another important step. However, given the worldwide structure of the cloud and the limits to enforcement of rules beyond borders, EU regulators will likely find some limits on enforcement and compliance rules they place on CSPs.[194]

As cloud consumers begin to entrust more and more personal data to the cloud, the risks that cloud computing poses will only increase. There is no place where the old idiom "you can't un-ring a bell" is truer than on the Internet. Lost, repurposed, or republished data is not recoverable in the traditional sense. Information is now copied, saved, stored, and reused in ways that were simply not possible pre-Internet. Cloud computing is often compared to utilities like electricity or water. In most states, governments regulate important utilities, at least to some extent. Resources that are of high importance for the national economy, even those operated privately, require some oversight. The cloud is no

---

191. Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 205 (2013) ("The law has generally adopted a restrained approach to technology regulation because of the rapid evolution of internet business models, traditionally deferring to business partners' privately ordered arrangements through contract as defining the relationship.").

192. *Id.*

193. Gleeson & Walden, *supra* note 94, at 25-31 (providing a list of general and cloud specific standards used in cloud computing (ISO2700 standards, Standards for Attestation Engagements No. 16 (SSAE 16), etc.)).

194. Rauhofer & Bowden, *supra* note 26, at 8 (questioning the ability of an EU data subject to bring a claim against a CSP outside of the EU in an EU court and receive any compensation from a CSP without assets in the EU).

different. Laws requiring minimum contracting standards will not destroy cloud computing. In fact, the opposite is likely true.