Santa Clara University School of Law

Santa Clara Law Review

Volume 54 | Number 2 Article 6

6-2-2014

The Uncertain Future: Privacy and Security in Cloud Computing

James Ryan

THE UNCERTAIN FUTURE: PRIVACY AND SECURITY IN CLOUD COMPUTING

James Ryan*

TABLE OF CONTENTS

INTRODUCTION

Imagine a world without bulky desk-top computers, without the constant struggle to keep software up to date, and without overworked corporate IT departments struggling to keep systems minimally functional; this vision was given to the public when cloud computing first became a possibility. Cloud computing presents a potential paradigm shift for all sectors of society. Why then, have these technologies not taken the world by storm?

* J.D. Candidate, May 2014, Santa Clara University School of Law.

Despite the numerous technical benefits of cloud computing, consumers must consider the significant question of what legal rights and responsibilities these new technologies trigger. As with most new technologies, the applicability of existing laws, the possibility of new laws tailored specifically to the new technology, and the specter of future regulatory action, all remain unclear. Although the modern world is truly a global economy, and cloud computing touches virtually every corner of the globe, this Comment will focus on the differences between United States and European Union law to illuminate the difficulties facing the market for cloud computing.

These legal uncertainties pose significant risks to cloud service providers and consumers alike. Service providers' management structures are forced to balance the reward of investing in new technologies with the risks posed by lawsuits under existing laws and the distinct possibility that their firm will be exposed to significant new and unforeseeable liabilities under future laws and regulations. Large companies looking to utilize these new services must rely mostly on skilled contract writing, rather than clear industry or government enforced standards, to protect their rights and liabilities. Individuals and smaller companies, on the other hand, are essentially unable to negotiate and are thus subject to adhesion contracts with whatever terms the various service providers happen to include.

This Comment will demonstrate that the uncertainty caused by ambiguous enforcement of existing laws, a lack of clearly applicable regulations, and inconsistent industry standards regarding privacy and security concerns, result in a high degree of risk for the cloud computing industry. This uncertainty, in turn, suppresses both supply and demand. In order to establish the existence of uncertainty and the problems therein, I will discuss the applicable economic theory,[1] define cloud computing,[2] discuss the societal importance of the technology and law,[3] identify political players,[4] outline the applicable laws and regulations and

1. *See infra* Part I.A.
2. *See infra* Part I.B.
3. *See infra* Part II.
4. *See infra* Part I.C.

compare them on a broad level to European Union Law,[5] discuss industry standards and contracts,[6] and provide recommendations for future U.S. law regarding cloud computing.[7]

I. BACKGROUND

A. Underlying Economic Theory

A large portion of economic theory focuses on the function of efficient markets and the allocation of goods.[8] Italian economist Vilfredo Pareto developed the traditional definition of economic efficiency: a market or allocation of goods is "efficient if there is no other allocation which makes no one worse off while making some agents strictly better off."[9] The balancing that takes place in the context of this Comment is between producers and consumers. Producers' options are determined by the "sum of the values of the inputs minus the sum of the values of the outputs," and consumers allocate their resources such that "the present net worth of a consumer is the total value of his resources plus the total value of his shares of the present values of producers' production plans."[10] As such, there is a problem resulting from market participants' inability to accurately assess the present value of their goods (a problem of uncertainty).[11] These issues, due to regulatory and legal flux, exist in various industries.[12]

5. *See infra* Part I.D.
6. *See infra* Part I.E.
7. *See infra* Part IV.
8. One conception of economics is that it is the study of the allocation of scarce resources. The focus of academic thought is thus, generally, how to efficiently distribute those resources to maximize utility. *See, e.g.*, Herbert A. Simon, *Rationality as Process and as Product of Thought*, 68 AM. ECON. REV. 1, 1 (1978).
9. Thomas R. Palfrey & Sanjay Srivastava, *Bayesian Implementation*, *in* 53 FUNDAMENTALS OF PURE AND APPLIED ECONOMICS 13 (A. Postlewaite ed., 1993).
10. Roy Radner, *Problems in the Theory of Markets under Uncertainty*, 60 AM. ECON. REV. 454, 455 (1970).
11. *See* Louis K. C. Chan, Josef Lakonishok, & Theodore Sougiannis, *The Stock Market Valuation of Research and Development Expenditures*, 56 J. FIN. 2431, 2454 (2001) ("[T]he lack of accounting information on such an important intangible asset [R&D expenditure and expected value] may impose real costs on investors through increased volatility.").
12. *See id.*

While the actual market strategies of current players in the cloud computing industry are impossible to ascertain from the outside, uncertainty does have a common impact in other industries.[13] In the electricity industry, for instance, companies were found to reduce investment when the relevant legislators exhibited a lack of coherent direction on the regulatory front.[14] The analogy is clear: industries forced to balance risks and rewards attributable to regulatory unpredictability are expected to react in a similar fashion.[15] While there are no industries where a direct comparison can be made, an unexpected regulatory change in the nuclear power industry caused nuclear power providers to lose as much as ninety percent of their profits.[16] This possibility of a drastic shift as a result of changing regulatory schemes leaves the budding cloud computing industry in a state of inefficiency.

Essentially, firms pay close attention to the laws and regulations affecting the sustainability of their business model, and "when firms perceive that new regulatory initiatives are unstable, specific investments appear more risky."[17] This theory was borne out in the electricity industry where a new act increased investment significantly in states with little to no history of regulatory reversals, and had no statistically significant effect in states with a history of repealing regulatory acts.[18] In sum, when it comes to sunk costs[19] or transaction specific investments, "uncertainty is widely conceded to be a critical attribute."[20]

13. *See id.*

14. Kira R. Fabrizio, *The Effect of Regulatory Uncertainty on Investment: Evidence from the Renewable Energy Generation* 1 (The Wharton Sch., 11th Annual Strategy and the Business Environment Conference, 2011), *available at* http://www-management.wharton.upenn.edu/henisz/msbe/2011/4_2_Fabrizio.pdf.

15. *Id.*

16. *See* Arie Kapteyn, Nicholas Kieffer & John Rust, *Introduction The Microeconometrics of Dynamic Decision Making, Journal of Applied Econometrics*, 10 J APPLIED ECONOMETRICS S1, S5 (1995).

17. Fabrizio, *supra* note 14, at 2.

18. *See id.* at 3.

19. *Sunk Cost Definition*, MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/sunk%20cost (last visited Oct. 24, 2012) (defining sunk cost as "a cost already incurred that is not subject to variation or revision").

20. Oliver E. Williamson, *Transaction-Cost Economics: The Governance of Contractual Relations*, 22 J. L. & ECON. 233, 239 (1979).

This bears relevance to cloud computing in that any investment down a particular chain of technology or security software development is a sunk cost of operation. Unable to predict which specifications compliance with possible regulatory systems will entail, companies will simply not invest in any more technology than is necessary to remain competitive. In addition, in the modern legal climate, the cost of litigating lawsuits is significant for both service providers and the direct consumers. Moreover, these costs are unpredictable.

B. Technology

To understand the root of the issues, it is important to first be clear about what cloud computing actually entails.[21] Cloud computing has antecedents as early as the 1950s, when AT&T designed and developed centralized data storage systems for businesses.[22] Today, cloud computing has evolved to encompass a variety of information technology solutions.[23] The National Institute of Standards and Technology is the government body responsible for, among other things, establishing "assessment criteria and test data sets for validation of industrial products" in the information technology space.[24] The policy directive of this organization is to "foster cloud computing systems and practices that support interoperability, portability, and security."[25] In an attempt to provide a broad working definition, the NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction."[26]

21. This overview of the technology involved in cloud computing, while by no means exhaustive, should be sufficient to anticipate and understand many of the issues facing the industry.

22. *See A Complete History of Cloud Computing,* SALESFORCE, http://www.salesforce.com/uk/socialsuccess/cloud-computing/the-complete-history-of-cloud-computing.jsp (last visited Mar. 18, 2014).

23. *See NIST Cloud Computing Program*, NAT'L INST. OF STANDARDS & TECH.(Jan. 28, 2014), http://www.nist.gov/itl/cloud/index.cfm.

24. *What ITL Does*, NAT'L INST. OF STANDARDS & TECH. (Jan. 25, 2011), http://www.nist.gov/itl/what-itl-does.cfm.

25. *NIST Cloud Computing Program*, *supra* note 23.

26. PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (Sept. 2011), *available at* http://csrc.nist.gov/publications/

The definition proceeds to list five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[27] Self-service essentially provides "ability to upload, build, deploy, schedule, manage, and report . . . on demand."[28] Broad network access is defined as a system where "capabilities are available over the network and accessed through standard mechanisms."[29] Resource pooling entails "a standardized, scalable, and secure physical infrastructure"[30] that is used to serve multiple customers.[31] Rapid elasticity is simply the on-demand rapidly scalable nature of the pooled resources.[32] Finally, these systems employ measured service, meaning that there is "a metering capability which enables [parties] to control and optimize resource use."[33]

The five characteristics of cloud computing manifest into several broad categories of services offered: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).[34] SaaS providers install and run software on their servers which are accessed remotely by customers.[35] The most common SaaS services are Salesforce.com's online management tools.[36] IaaS services, such as Amazon's Elastic Compute Cloud,[37] offer flexibility and scalability by furnishing customers with access to virtual servers where the customer then installs and maintains their

nistpubs/800-145/SP800-145.pdf.

27. *Id.*

28. Dave Malcolm Surgient, *The Five Defining Characteristics of Cloud Computing | ZDNet*, VIRTULIZATION (Apr. 9, 2009), http://www.zdnet.com/news/the-five-defining-characteristics-of-cloud-computing/287001.

29. MELL & GRANCE, *supra* note 26, at 2.

30. Surgient, *supra* note 28.

31. MELL & GRANCE, *supra* note 26, at 2.

32. *Rapid Elasticity*, CLOUD BASED COMPUTING (Sept. 19, 2010), http://cloudglossary.com/home/id.Rapid-Elasticity/i.html.

33. *Essential Characteristics of Cloud Computing*, ISACA, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/Essential%20characteristics%20of%20Cloud%20Computing.pdf.

34. MELL & GRANCE, s*upra* note 26, at 2.

35. *Id.*

36. *See* Ania Monaco, *A View Inside the Cloud*, THE INSTITUTE (June 7, 2012), http://theinstitute.ieee.org/technology-focus/technology-topic/a-view-inside-the-cloud.

37. *Amazon EC2*, AMAZON WEB SERVICES, aws.amazon.com/ec2 (last visited Feb. 27, 2014).

own software.[38] Finally, PaaS options such as the Google App Engine have aspects of both of the preceding branches in that they use an entire platform hosted on the provider's server, often including everything from an operating system to developer tools.[39]

These service models are then divided into three broad types of implementation.[40] Public cloud services have no local infrastructure, and are shared among multiple customers.[41] Private clouds entail an infrastructure used by a single organization that can be owned or managed either by that organization or a third party.[42] Hybrid clouds are, as the name suggests, a combination of the above and characterized by "standardized or proprietary technology that enables data and application portability."[43]

C. The Political Players

Due to the vast amount of money involved and the growing importance of the technology,[44] the United States government has no choice but to take notice of the cloud computing industry.[45] The Congressional Subcommittee on Intellectual Property, Competition, and the Internet is the primary entity responsible for regulations regarding Internet-based technologies.[46] This committee only recently began

38. *See* MELL & GRANCE, *supra* note 26, at 3.
39. *See id.* at 2–3.
40. *See id.* at 3.
41. *See id.*
42. *Id.*
43. *Id.*
44. *See* Joe McKendrick, *Cloud Computing Market Hot, but How Hot? Estimates are All Over the Map*, FORBES (Feb. 13, 2012), http://www.forbes.com/sites/joemckendrick/2012/02/13/cloud-computing-market-hot-but-how-hot-estimates-are-all-over-the-map/.
45. *See generally Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearing Before the Subcommittee on Intellectual Property, Competition, and the Internet*, 112th Cong. 112–122 (2012) [hereinafter *Cloud Computing Hearing*]. Acknowledging both the committee's lack of knowledge and the importance of this burgeoning industry, the ranking member of the subcommittee quipped that the hearing "is an important hearing about things in the cloud, which some people say that is where I always am. So I want to figure out what is going on up there." *Id.* at 2 (statement of Rep. Melvin L. Watt, ranking member, Subcommittee on Intellectual Property, Competition, and the Internet).
46. *See Subcommittee on Intellectual Property, Competition, and the Internet*, U.S. HOUSE OF REPS. JUDICIARY COMM., http://judiciary.house.gov/index.cfm/subcommittee-on-courts-intellectual-property-and-the-internet (last

discussing the future of cloud computing in earnest.[47] Prior to this hearing, and continuing for the time being, the laws and regulations regarding cloud computing are mostly handled by whichever agency regulates the particular industry sector purchasing the cloud service.[48] This means that privacy law comes in various parts from the Federal Trade Commission Act,[49] the Electronic Communications Privacy Act (specifically the Stored Communications Act),[50] the Health Insurance Portability and Accountability Act,[51] and the Fair Credit Reporting Act,[52]rather than from a centralized regulation governing cloud computing itself.[53] Although, to date, only that particular subcommittee has shown significant interest, the amount of money involved suggests that other governmental agencies such as the FCC or FTC may show more interest in the future.[54] Piecemeal regulatory action leaves the political players unable to realize their policy goals and companies subject to illogical and unpredictable policies meant for other industries and technologies.

States in the European Union, on the other hand, tend to have non-cloud specific but otherwise comprehensive plans in place that correspond to the E.U. Data Protection Directive.[55] Only as recently as the summer of 2012, however, have E.U. officials clarified their plans for specific cloud computing regulations (still significantly ahead of the Congressional

visited Feb. 28, 2014). "The *Subcommittee on Intellectual Property, Competition, and the Internet* shall have jurisdiction over the following subject matters: copyright, patent, trademark law, information technology, antitrust matters, other appropriate matters as referred by the Chairman, and relevant oversight." *Id.* (emphasis added).

47. This hearing was held on July 25, 2012. *Cloud Computing Hearing*, *supra* note 45.

48. *See* BUS. SOFTWARE ALLIANCE, BSA GLOBAL CLOUD COMPUTING SCORE CARD 12 (2012), *available at* http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf.

49. 15 U.S.C. §§ 41–58 (2012).

50. 18 U.S.C. §§ 2701–12 (2012).

51. Health Insurance Portability and Accountability Act (HIPPA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.).

52. 15 U.S.C. § 1681 (2012).

53. BUS. SOFTWARE ALLIANCE, COUNTRY REPORT: UNITED STATES 1 (Feb. 22, 2012), *available at* http://portal.bsa.org/cloudscorecard2012/assets/pdfs/country_reports/Country_Report_US.pdf.

54. *See* McKendrick, *supra* note 44.

55. *See* BUS. SOFTWARE ALLIANCE, *supra* note 48, at 13–15.

subcommittee which only recently began to consider cloud computing issues).[56] Even among states in compliance with the E.U. Data Protection Directive, however, there are "differing national legal frameworks and uncertainties over applicable law."[57] As such, the European Commission's vice president, Neelie Kroes, is leading the effort to devise a standardized set of laws and regulations that can be applied to cloud computing across the European Union.[58]

While there are a great number of politicians and regulatory bodies with an interest in cloud computing, the European Commission and the Congressional Subcommittee on Intellectual Property, Competition, and the Internet are the two most likely to play a major role in the future regulatory and legal framework.

D. The Legal and Regulatory Climate in the United States and European Union

There are two primary models for dealing with privacy and security issues: piecemeal regulation issue by issue,[59] and attempts to regulate cloud computing directly.[60] The first approach represents the United States' current model where the second represents the approach the European Union is moving towards. Rather than the standard voluntary uptake for E.U. regulations, the new European Union data law will require compliance by all member states and firms acting within the region.[61] A one hundred and nineteen page

56. *See* Press Release, Eurpora, *Digital Agenda: New strategy to drive European business and government productivity via cloud computing* (Sept. 27, 2012), *available at* http://europa.eu/rapid/press-release_IP-12-1025_en.htm.

57. EUROPEAN COMM'N, UNLEASHING THE POTENTIAL OF CLOUD COMPUTING IN EUROPE 5 (Sept. 27, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

58. *See* Barb Darrow, *Europe Cloud Plan Addresses Data Protection Problem. Sort of.*, GIGAOM (Sept. 27, 2012), http://gigaom.com/cloud/ec-cloud-plan-addresses-data-protection-problem-sort-of/.

59. *See generally*, Roland L. Trope & Sarah Jane Hughes*, Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WILLAMETTE L. REV. 111 (2011) (the author differentiates among issues stemming from cloud computing systems and evaluates them separately).

60. *See, e.g.*, *New Draft European Data Protection Regime,* LAW PATENT GRP. (Feb. 2, 2012), http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227 (describing the new European approach to data protection in the cloud).

61. *See* Tom Espiner*, Firms Face Tough New EU Fines for Data Breaches,* ZDNET (Jan. 25, 2012), http://www.zdnet.com/firms-face-tough-new-eu-fines-for-

document details the layout of the coming legislation.[62] The European Union's data law seeks to achieve easier data portability between service providers, a single set of rules across borders, and the requirement that personal data handled by foreign companies be subject to the same regulations.[63] The following subsections will cover most of the applicable laws and regulations currently applied to cloud computing in the United States.

1. Applicable Regulatory Frameworks

There are a large number of state and federal laws and regulations that could be applied to cloud computing.[64] Ignoring various state laws, there are nine widely applicable sets of regulations, at least six industry-specific guidelines and requirements, and a variety of international laws with bearing on U.S. companies just in the data security space.[65] Foremost among these, at least in terms of visibility, are the Stored Communications Act,[66] the Patriot Act,[67] the Health Insurance Portability and Accountability Act,[68] export regulations overseen by the Departments of Commerce and State,[69] and consumer protection under the FTC.[70]

---

data-breaches-3040094907/.

62. European Commission Proposal, *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),* 2012/0011 (COD) (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter European Commission Proposal].

63. *See* Press Release, Eurpora, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

64. *See* Jason Bloomberg, *Cloud Computing: Legal Quagmire*, ZAPTHINK (Jul. 5, 2011), http://www.zapthink.com/2011/07/05/cloud-computing-legal-quagmire/.

65. *The Security Laws, Regulations and Guidelines Directory*, CSO SECURITY & RISK (Dec. 19, 2012), http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory.

66. 18 U.S.C. §§ 2701–12 (2012).

67. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8 U.S.C., 12 U.S.C., 15 U.S.C., 18 U.S.C., 20 U.S.C., 31 U.S.C., 42 U.S.C., 47 U.S.C., 49 U.S.C., and 50 U.S.C.) (2001).

68. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.).

69. 15 C.F.R. § 732 (2011).

70. For a tabulation of cloud computing security laws, regulations, and

The Stored Communications Act (SCA) is rooted in the Electronic Communications Privacy Act of 1986 (ECPA).[71] In determining whether a particular type of computer network usage falls under the SCA, the data must be either an electronic communication service (handling data transmissions and electronic mail) or a remote computing service (providing outsourced computer processing and data storage).[72] The significance of this distinction is that the protection afforded to stored data (RCS) is lower than the protection afforded to the transmitting data (ECS).[73] Different courts do not have a consensus as to categorizing these services.[74] In *Quon v. Arch Wireless*,[75] the Ninth Circuit ruled that because the back-up of text messages was incidental to the provision of the messaging service, they would be classified as an ECS.[76] The holding in the *Theofel v. Farey-Jones*[77] case, also from the Ninth Circuit, illustrates that the boundary between RCS and ECS is essentially arbitrary; holding that even indefinite e-mail backup storage constitutes an ECS service provision.[78] For the purposes of this Comment, the exact line drawn between RCS and ECS is less important than the fact that the "ECPA has been outpaced" by technological progress.[79] What is important is that this antiquated statute, written in 1986, is an exceedingly poor fit for today's technology and woefully inadequate going forward.

Another visible concern for the cloud computing industry is the U.S. Patriot Act.[80] The data security implication of the

guidelines as of 2012 *see The Security Laws, Regulations and Guidelines Directory*, *supra* note 65.

71. *Electronic Communications Privacy Act of 1986*, EFF (Oct. 21, 2005), http://ilt.eff.org/index.php/Category:ECPA.

72. William Jeremy Robinson, Note, *Free at What Cost? Cloud Computing Privacy under the Stored Communications Act,* 98 GEO. L.J. 1195, 1205 (2010).

73. *See* Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. ON TELECOMM. & HIGH TECH. L. 53, 84 (2012).

74. *See id.* at 87.

75. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *rev'd and rem'd sub. nom*. City of Ontario v. Quon, 560 U.S. 746 (2010).

76. *Id.* at 901.

77. Theofel v. Farely-Jones, 359 F.3d 1066, 1072 (9th Cir. 2003).

78. *Id.*

79. *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Mar. 18, 2014).

80. *See* David Saleh Rauf, *PATRIOT Act Clouds Picture for Tech,* POLITICO

Patriot Act is that companies can be forced to turn over data to the U.S. government, even without notice to the customer.[81] Furthermore, even data stored outside U.S. borders, if held in servers owned by a U.S. company, can potentially be compromised.[82] The Patriot Act is so powerful that even contract provisions specifying that data will be governed by foreign law can be ignored by the U.S. government.[83] Specifically, section 215 of the Patriot Act allows the FBI to access data related to investigations in an *ex parte* proceeding with the requirement that "no person shall disclose to any other person . . . that the [FBI] has sought or obtained things under this section."[84] The ramifications of the Patriot Act are directly pressing for consumers, and thereby concerning to providers looking to increase uptake.

One statute that is familiar to most is the Health Insurance Portability and Accountability Act (HIPAA). HIPPA provides standards that must be followed for companies dealing with health information.[85] The act requires that most people who maintain or transmit "health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards."[86] The responsibilities to comply with obligations, such as HIPAA, pose another major burden because customers cannot avoid liability simply by delegating information technology to a cloud vendor.[87] Thus, a need exists for detailed contracting to apportion indemnification.[88] In the absence of such a

(Nov. 29, 2011), http://www.politico.com/news/stories/1111/69366.html.

81. Amar Toor, *Microsoft: European Cloud Data May Not be Immune to the Patriot Act,* ENGAGET (Jun. 30, 2011), http://www.engadget.com/2011/06/30/microsoft-european-cloud-data-may-not-be-immune-to-the-patriot/.

82. Amar Toor, *Microsoft's Patriot Act Admission Has the EU Up in Arms*, ENGAGET (Jul. 6, 2011), http://www.engadget.com/2011/07/06/microsofts-patriot-act-admission-has-the-eu-up-in-arms/.

83. Zack Whittaker, *Case Study: How the USA Patriot Act Can be used to access EU Data*, ZDNET (Apr. 26, 2011), http://www.zdnet.com/blog/igeneration/case-study-how-the-usa-patriot-act-can-be-used-to-access-eu-data/8805.

84. 50 U.S.C. § 1861(d)(1).

85. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.).

86. 42 U.S.C. § 1320d-2(d)(2).

87. *See* H. Ward Classen, *Cloudy with a Chance of Rain: Avoiding Pitfalls in Cloud Computing,* 45 MD. B. J. 18, 23 (2012).

88. *See id.*

contract, the customer may suffer for a data breach that is the fault of the provider.[89] Due to the lack of industry certifications that would establish this reasonable standard, even thorough contracting cannot entirely ensure that there will not be "a number of people with access to the physical servers and storage" and "end-to-end" encryption.[90] HIPAA violations can be severe with penalties including hefty fines and imprisonment.[91] The Health Information Technology for Economic and Clinical Health Act sets out punishment ranging from $100 fines for violations deemed accidental to as much as $50,000 for each instance of a breach due to willful neglect.[92] Additionally, attorneys' fees and other costs may now be sought.[93]

In addition to HIPAA's regulations based on the personal privacy of information, the Bureau of Industry and Security (BIS) regulates based on the content of the information transmitted in the cloud.[94] The BIS has assured cloud providers that they do not need to obtain export licenses for foreign information technology for clients who utilize their services, at least when the provider is not transmitting data to the user.[95] There is, however, less guidance regarding how the Department of Commerce would handle a U.S. company uploading controlled information.[96] The BIS' regulations, detailed in the Export Administration Regulations,[97] define controlled information as content related to nuclear materials facilities and equipment, chemicals, microorganisms, toxins, materials processing, electronics,

89. *See id.*

90. Chris Witt, *HIPAA vs the Cloud,* HEALTHCARE IT NEWS (Sept. 9, 2011), http://www.healthcareitnews.com/news/hipaa-vs-cloud.

91. *HIPAA and the HITECH Act: Know the Level of Penalties*, HC PRO (Mar. 16, 2009), http://www.hcpro.com/HIM-229707-866/HIPAA-and-the-HITECH-Act-Know-the-level-of-penalties.html.

92. *Id.*

93. *Id.*

94. 15 C.F.R. § 732.2 (2011).

95. Letter from C. Randall Pratt, Director, Info. Tech. Controls Div., to redacted recipient (Jan. 11, 2011).

96. *See* Chad Breckinridge, *From the Experts: Cloud Computing's Hidden Export Regulation Risks*, CORP. COUNSEL (Feb. 27, 2012), http://www.wiltshiregrannis.com/siteFiles/News/6277E4F5146A461D9AFB1782C6E0C9E1.pdf.

97. *Export Administration Regulation Downloadable Files,* U.S. DEP'T OF COMMERCE, www.bis.doc.gov/policiesandregulations/ear/index.htm (last visited Mar. 1, 2014).

computers, telecommunications, information security, sensors and lasers, navigation and avionics, marine, and aerospace and propulsion.[98] The clearest example is saving technical plans to cloud storage where the storage center happens to be overseas; due to strict liability under EAR, the company could be subject to a $250,000 penalty per instance.[99] One cloud service provider (specifically virtualization software), VMware, is aware of the risks of export/re-export laws and regulations and has published an Export Control Policy, warning potential customers about the applicable regulations.[100] The combined lack of guidance and industry caution further limits the uptake of cloud computing.

Another possible source of regulatory oversight comes from the Federal Trade Commission (FTC).[101] A "security researcher" filed a complaint with the FTC regarding allegedly false claims about data protection.[102] The complaint alleged both that Dropbox, an online data storage solution, did not utilize industry best practices and that they made deceptive statements about the level of protection offered.[103] As of yet, there have been no further proceedings in the Dropbox case, leaving the FTC's desire to exercise authority in these situations unclear.

2. European Union Safe Harbor

Compliance with the safe harbor regulations is one of the only feasible ways United States cloud providers are currently able to compete in the European market.[104] These regulations were developed between the United States and

98. *Id.*

99. Breckinridge, s*upra* note 96.

100. *Export Control Policy*, VMWARE, http://www.vmware.com/help/export-control.html (last visited Mar. 18, 2014).

101. 15 U.S.C. § 45 (2012).

102. INFOSEC ISLAND, *Dropbox Responds to FTC Complaint about Data Security* (May 18, 2011), http://www.infosecisland.com/blogview/13848-Dropbox-Responds-to-FTC-Complaint-about-Data-Security.html.

103. Request for Investigation and Complaint for Injunctive Relief at 1, In the Matter of Dropbox, Inc. (FTC, May 11, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/05/dropbox-ftc-complaint-final.pdf.

104. *See* Patrick Van Eecke, *Cloud Computing Legal Issues*, DLA PIPER, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf (last visited Mar. 3, 2014).

European Union to "provide a streamlined means for U.S. organizations to comply with the Directive."[105] Among the terms of the Safe Harbor provisions are standards for the legitimate use of data, as well as for both the security and safety of data.[106] While these standards are technically self-administered, the FTC has stepped in under the umbrella of deceptive trade practices when U.S. companies fall short on their promises to their customers to comply with safe harbor standards.[107] If and when the proposed European Union framework for data security comes into effect, those reforms will essentially replace the Safe Harbor regulations and force U.S. companies to be certified under E.U. law—the exact specifications of which are currently unknown.[108] Regardless, the standards would not prevent privacy intrusions under the Patriot Act for companies owned or operating in the United States.[109]

E. Torts and State Law in the Cloud

In addition to formal regulatory frameworks, providers also face regulation from state laws and general tort principles.[110] The case of *Wong et. al. v. Dropbox, Inc.*,[111] is illustrative of possible state and tort principles faced by cloud providers: (1) Violation of the California Unfair Competition Law, Business & Professions Code section 17200, *et seq.*, (2) Invasion of Privacy—Intrusion, Public Disclosure of Private Facts, Misappropriation of Likeness and Identity, and

105. *Welcome to the U.S.-E.U. Safe Harbor*, EXPORT.GOV (Apr. 11, 2012), http://export.gov/safeharbor/eu/eg_main_018365.asp.

106. Zack Whittaker, *Safe Harbor: Why EU Data Needs 'Protecting' from US Law*, ZDNET (Apr. 25, 2011), http://www.zdnet.com/blog/igeneration/safe-harbor-why-eu-data-needs-protecting-from-us-law/8801.

107. *See* Anita Ramasastry, *The EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices,* FIND LAW (Nov. 17, 2009), http://writ.news.findlaw.com/ramasastry/20091117.html.

108. Zack Whittaker, *European Data Protection Law Proposals Revealed*, ZDNET (Dec. 7, 2011), http://www.zdnet.com/blog/london/european-data-protection-law-proposals-revealed/1365.

109. *See* Peter Cartier, *USA Patriot Act and Cloud Hosting: What You Need to Know*, FPWEB.NET (Jan. 16, 2012), http://blog.fpweb.net/usa-patriot-act-cloud-hosting/.

110. *See, e.g.*, James R. Hood, *Cloud Site Dropbox Drops the Ball*, CONSUMERAFFAIRS (June 27, 2011), http://www.consumeraffairs.com/news04/2011/06/cloud-site-dropbox-drops-the-ball.html.

111. Class Action Complaint, Wong v. DropBox, Inc., No. 4:11-cv-03092 (N.D. Cal. 2011), 2011 WL 9162340.

California Constitutional Right to Privacy, (3) Negligence, (4) Breach of Express Warranty, and (5) Breach of Implied Warranty.[112] The action against Dropbox arose out of an update that inadvertently allowed anyone to log into any account using any password. This security breach lasted approximately four hours.[113] In other data breach cases, the average award per plaintiff upon settlement was $2,500.[114] That means that in cases such as the 2011 PlayStation Network breach, where Sony lost approximately $171 million directly from the breach, companies also risk losing (through settlement or litigation) an additional $2,500 for each of their potentially millions of customers.[115] Although many cases are dismissed for failure to prove actual damages,[116] in at least one case of stolen electronic payment data, the court allowed mitigation damages for credit card replacement costs and credit insurance.[117]

F. Fourth Amendment and the Cloud

Another source of legal complexity is the applicability of the Fourth Amendment to cloud computing. The Fourth Amendment protects the right for people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[118] Supreme Court jurisprudence in the area is dominated by the test from *Katz v. United*

112. *Id.* at *1.

113. Matthew Humphries, *Dropbox Facing Class Action Lawsuit over "any password worked" Glitch*, GEEK (Jun. 28, 2011), http://www.geek.com/articles/geek-pick/dropbox-facing-class-action-lawsuit-over-any-password-worked-glitch-20110628/.

114. *Data Breach Costs Skyrocket as Class-Action Lawsuits become More Prevalent,* INFOSECURITY MAG. (Oct. 26, 2012), http://www.infosecurity-magazine.com/view/29022/data-breach-costs-skyrocket-as-classaction-lawsuits-become-more-prevalent/.

115. *Sony Data Breach Lawsuit Largely Dismissed*, INFOSECURITY MAG. (Oct. 23, 2012), http://www.infosecurity-magazine.com/view/28945/sony-data-breach-lawsuit-largely-dismissed.

116. David Navetta, *Federal Appeals Court Holds Identity Theft Insurance/Credit Monitoring Costs Constitute "Damages" in Hannaford Breach Case*, INFO. LAW GRP. (Oct. 24, 2011), http://www.infolawgroup.com/2011/10/articles/damages/federal-appeals-court-holds-identity-theft-insurancecredit-monitoring-costs-constitute-damages-in-hannaford-breach-case/.

117. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162–68 (1st Cir. 2011) (holding that, when confidential data is stolen by a third party the customers of a grocery, there is no confidential relationship but that there is a possibility of mitigation damages under negligence and implied contract theories).

118. U.S. CONST. amend. IV.

States.[119] In *Katz*, the Court recognized that people have a "reasonable expectation of privacy"[120] when two conditions are met: "First that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[121] The impact of the Fourth Amendment in cloud computing circumstances is unclear, as detailed below.[122]

II. THE SOCIETAL IMPORTANCE OF CLOUD COMPUTING

Cloud computing technologies represent a paradigm shift for both individuals and corporations.[123] These services take advantage of the principles of economies of scale and specialization to provide a more efficient solution for many information technology problems.[124] As in all situations, consumers on both the corporate and personal level will balance the risk with the reward of utilizing the new set of technologies. The primary risks are confusion as to applicable laws, the changing regulatory climate, and lack of industry standards.[125] While these risks can be quite significant depending on the profile of the consumer, there are a plethora of reasons why both corporations and individuals consider switching to the cloud. The problem is that despite the many benefits of cloud computing, the technology and society's benefit are being limited by the current legal structure.

The primary reason a corporation would be interested in utilizing cloud technology is that they no longer are responsible for maintaining their own information technology structure and can focus on their core competencies.[126] A close second in primacy is that the scalability of cloud computing

119. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
120. *Id.*
121. *Id.* at 361.
122. *See* i*nfra* Part I.F.
123. *See Cloud Computing Hearing*, *supra* note 45 (statement of Mr. Smith).
124. *See* Ryan Nichols, *Cloud Computing by the Numbers: What do All the Statistics Mean?*, COMPUTERWORLD (Aug. 31, 2010), http://blogs.computerworld.com/16863/cloud_computing_by_the_numbers_what_do_all_the_statistics_mean.
125. *See infra* Part II.
126. *See* Janakiram MSV, *Top 10 Reasons Why Startups Should Consider Cloud Computing,* YOUR STORY (Jul. 20, 2012), http://cloudstory.in/2012/07/top-10-reasons-why-startups-should-consider-cloud/.

allows companies to only pay for computing power when they actually need it.[127] That is, instead of having a large server farm running all of the time, even in low traffic periods, companies pay as needed on a virtually instantaneous basis.[128] Various analysts suggest that the market for cloud computing will grow rapidly.[129] In fact, current estimates from Forrester state that the market will reach two hundred and forty one billion dollars by the year 2020.[130] This is in large part due to the fact that estimates suggest savings due to virtualization can "[cut] the cost of computing by up to 50 percent with savings gains from lower infrastructure operational costs."[131] At the moment, however, many enterprises only look to cloud computing when "deploying new, non-mission-critical apps or apps not containing sensitive data."[132] These mission critical or highly sensitive applications are also those subject to the highest levels of investment, meaning that they have the largest margin for improvements in efficiency.[133]

There are, of course, also non-legal risks associated with utilizing cloud computing.[134] Some of the more threatening aspects of cloud computing implementation are the large attack surface,[135] shared multi-tenant environments,[136] loss of

127. *See Cloud Computing Hearing*, *supra* note 45 (statement of Mr. Smith).

128. *Id.*

129. Nichols, *supra* note 124.

130. Rick Blaisdell, *Cloud Computing Market Size—Facts and Trends,* CLOUDTWEAKS (Jul. 7, 2012), http://www.cloudtweaks.com/2012/07/cloud-computing-market-size-facts-and-trends/.

131. *See Cloud Computing Hearing*, *supra* note 45 (statement of Mr. Castro).

132. Derrick Harris*, It's Cloud Prediction Time: IDC, Gartner (and I) Weigh in,* GIGAOM (Dec. 1, 2011), http://gigaom.com/cloud/its-cloud-prediction-time-idc-gartner-and-i-weigh-in/.

133. *See* Archana Venkatraman, *CIOs Distrust Public Cloud for Mission-Critical Work, Says IDC*, COMPUTER WEEKLY (Nov. 9, 2012), http://www.computerweekly.com/news/2240170818/CIOs-distrust-public-cloud-for-mission-critical-work-says-IDC.

134. *See, e.g.*, *Cloudy With a Chance of Rain*, THE ECONOMIST (Mar. 5, 2010), http://www.economist.com/node/15640793 ("What is holding IT managers back is fear about security.").

135. *See* PRATYUSA K. MANADHATA, YUECEL KARABULUT & JEANNETTE WING, CARNEGIE MELON UNIV., REPORT: MEASURING THE ATTACK SURFACES OF ENTERPRISE SOFTWARE 3 (2008), *available at* http://www.cs.cmu.edu/~wing/publications/ManadhataKarabulutWing08.pdf. The authors define attack surface in terms of the number of entry and exit points of data, the number of channels and set of untrusted data times (terms also defined in the article). *Id.*

136. JUNIPER NETWORKS, SECURING MULTI-TENANCY AND CLOUD COMPUTING 3 (Mar. 2012), *available at* http://www.juniper.net/us/en/local/pdf/

control over data, and Internet-facing clients.[137] Aside from the technical problems companies face, there is awareness in the industry that certain regulatory mandates can pose risks for failure to properly secure data.[138]

In fact, at this point, it seems that decision makers are not seeing the value in cloud computing. According to some analysts, the attitude regarding cloud computing is heading from hype to disillusionment.[139] One IBM survey suggests that "only 13% of businesses have substantially implemented any cloud based services."[140] Nevertheless, other analysts predict that between 2011 and 2014, as a percentage of total applications used by corporations, cloud computing will double in Europe and go up by roughly seventy nine percent in the United States and Asia.[141] The European Union already has a more predictable set of regulations, yet IDC predicts that further policy driven change could greatly increase adoption going forward.[142] The perception at the moment is that contracts tend to favor service providers, and that it is impractical (if not essentially impossible) to verify if the contracted-for security precautions have in fact been provided until after a breach occurs.[143]

---

whitepapers/2000381-en.pdf. The authors define multi-tenancy as a system where many tenants share the same resources such as hardware, servers, data storage devices, and even applications. *Id.*

137. *See* WAYNE JANSEN & TIMOTHY GRACE, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING vii–viii (Dec. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

138. *See Cloudy With a Chance of Rain, supra* note 134.

139. *See* Derek du Preez, *Gartner: Cloud Uptake Lower than Expected*, COMPUTERWORLDUK (Aug. 17, 2012), http://www.computerworlduk.com/news/it-business/3376477/gartner-cloud-uptake-lower-than-expected/.

140. *IBM Find Businesses Slow on Uptake of Cloud Computing*, IBSI IN[N]OVATIVE BUS. SYS. (Apr. 7, 2012), http://www.ibsi-us.com/2012/04/ibm-find-businesses-slow-on-uptake-of-cloud-computing/#comments.

141. *The State of Adoption of Cloud Applications*, TATA CONSULTANCY SERVS., http://sites.tcs.com/cloudstudy/the-state-of-adoption-of-cloud-applications#.UI2frHf9cz5 (last visited Mar. 18, 2014).

142. DAVID BRADSHAW ET AL., QUANTITATIVE ESTIMATES OF THE DEMAND FOR CLOUD COMPUTING IN EUROPE AND THE LIKELY BARRIERS TO UP-TAKE 9 (Jul. 13, 2012), http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf ("[P]olicy actions aimed at removing barriers to cloud can have a relevant impact on its adoption, increasing the value of spending on public clouds from €35 billion (No intervention scenario) to almost €80 billion (Policy-driven scenario) by 2020.").

143. Gregory Musungu, *Treading Carefully with Cloud Computing Solutions, Contracts, and Services*, CLOUDTWEAKS (Oct. 2, 2012), http://www.cloudtweaks.com/2012/10/treading-carefully-with-cloud-computing-

These contractual issues and inability to self-regulate are magnified when it comes to individual utilization of cloud computing services. The American public is an odd mix of highly competent and well informed consumers, with a significant portion of the population who believe that "cloud technology is linked with weather, has kinship with heaven, is closely related to happenings in the outer galaxy and even has something to do with toilet paper (huh?)."[144] The knowledge issue is relevant because although about sixty percent of respondents claimed they had not used cloud computing services, something closer to ninety five percent were actually using services with cloud computing components.[145] This means that a significant portion of the public is unwittingly exposed to unknown degrees of liability.[146] While organizations and corporations are advised to negotiate their own contracts and terms of service, a non-negotiable service agreement is the standard in publicly available cloud computing.[147] These adhesion contracts include clauses such as jurisdictional choice, time limits in which claims can be brought, and other clauses that severely limit the rights of those consumers unable to effectively negotiate.[148] Regardless, many consumers do choose to assume the risk (or, more likely, remain unaware of said risk) and use at least some cloud computing services.

III. ANALYSIS

A. The Effects of the Regulatory Quagmire

In many respects, the maze of laws and regulations facing the cloud computing industry, even limited to the topic of privacy and security, act as a veritable sword of

solutions-contracts-and-services/.

144. Humayun Shahid, *Cloud Confusion: The 'Fluffy White Thing' and the Potential Within*, CLOUDTWEAKS (Sept. 4, 2012), http://www.cloudtweaks.com/2012/09/cloud-confusion-the-fluffy-white-thing-and-the-potential-within/.

145. *Id.* Examples of these services given are "online banking, purchasing goods online, being socially connected, enjoying online games." *Id.*

146. *See infra* Part III.C for a discussion of industry standards.

147. *See* JANSEN & GRACE, *supra* note 137, at vii.

148. *See* 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, 198–214 (2011).

Damocles.[149] Each of the following regulatory schemes (detailed earlier)[150] create their own problems for consumers and providers wishing to act in the cloud computing space.

The major problem with the Stored Communications Act is the disagreement regarding which services belong in which category.[151] The logic of applying the SCA to current cloud computing is also strained because the original act was based on the theory that consumers were entrusting their data in an agency-like relationship, whereas most see cloud computing as more akin to a rental locker.[152] While more than a civil subpoena is required to obtain more than basic subscriber information,[153] information must fall into one of several categories in order for it to be protected by the requirement that the government obtain a search warrant.[154] Regardless of any particular court's decision, the SCA is outdated.[155] Despite the twenty-five years of inaction, and support from most of the major players in the industry,[156] legislation to update the protection of e-mail and other electronic data has only recently been introduced.[157] While

149. N.S. Gil, *What is the Sword of Damocles?*, CLASSICAL HISTORY, http://ancienthistory.about.com/od/ciceroworkslatin/f/DamoclesSword.htm (last visited Mar. 3, 2014).

150. *See supra* Part I.D–F.

151. *Compare* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901 (9th Cir. 2008) (holding that because the primary service of defendant was communication provision, the storage of that data was incidental), *with* Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004) (holding that even though the ISP's purpose was not necessarily the sending of data, it still fell within ECS protection).

152. *See* Hien Timothy M. Nguyen, Note, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing,* 86 NOTRE DAME L. REV. 2189, 2205–06 (2011).

153. Fed. Trade Comm'n v. Netscape Commc'ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000).

154. Disclosure may be required following a subpoena if the information is the contents of wire or electronic communications in electronic storage, contents of wire or electronic communications in a remote computing service, or records concerning ECS or RCS. 18 U.S.C. §§ 2703(a)–(c) (2012).

155. Declan McCullagh, *Google, Facebook go Retro in Push to update 1986 Privacy Law*, CNET (Oct. 21, 2011), http://news.cnet.com/8301-31921_3-20123710-281/google-facebook-go-retro-in-push-to-update-1986-privacy-law/.

156. *See Who We Are*, DIGITAL DUE PROCESS, http://digitalddueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Mar. 18, 2014).

157. *See* Chris Calabrese, *Email Privacy Faces a Key Test Next Week*, FREE FUTURE (Sept. 11, 2012), http://www.aclu.org/blog/technology-and-liberty-national-security/email-privacy-faces-key-test-next-week.

opponents argue that warrant-level protection would hinder law enforcement efforts, the proposed legislation would go a long way toward easing the minds of both sides of the cloud computing market.[158]

Aside from SCA protection of electronic data, the Patriot Act poses the biggest challenge to U.S. companies.[159] Less important than the actual content of the law, however, is the uncertainty created by it. This reality leads to "no shortage of people who misapprehend the law. If some of these misperceptions harden or real problems [are] not addressed, it will cause companies and governments to hesitate in doing business with U.S. cloud companies."[160] Specifically, an issue admittedly more of public relations than legal jurisprudence, many other countries' data protection laws "provide governments with 'expedited access' to Cloud data."[161] In a very real sense, however, the Patriot Act undermines much of the importance of the debate regarding the SCA because, unlike other laws, it is a legal burden that cannot be contracted around.[162]

While the SCA and Patriot Act create doubt over the viability of data protection, other regulatory schemes create other problems. The HIPPA,[163] EAR,[164] and possible FTC proceedings for deceptive trade practices,[165] all create a significant risk for both providers and customers of cloud services leading to higher transaction costs and more complicated contracts.[166] While there are no outstanding cases under the EAR code sections, the government has not yet offered any guidance either way whether they will offer

158. *See generally* McCullagh, *supra* note 155 (discussing, among other things, the lack of bipartisan support and opposition of the U.S. Justice Department).

159. *See* Aidan Finn, *A Factual Analysis of Cloud Computing VS the USA Patriot Act*, AIDAN FINN, IT PRO BLOG (Apr. 26, 2011), http://www.aidanfinn.com/?p=11187 ("[I]f data laws continue to cause concern then what's to stop a Chinese operator dominating there, or a French/UK/German operator dominating in Europe. . . .").

160. Rauf, *supra* note 80.

161. Gery Menegaz, *Bad Assumptions about Cloud Computing and the Patriot Act*, ZDNET (Aug. 17, 2012), http://www.zdnet.com/bad-assumptions-about-cloud-computing-and-the-patriot-act-7000002614/.

162. *See* Musungu, *supra* note 143.

163. *See supra* Part I.D.

164. *See id.*

165. *See id.*

166. *See id.*

clarification or begin enforcing EAR strictly.[167] The risk of being faced with an FTC proceeding is an outstanding issue that cannot be discounted. Due to the fact that fines and prosecutions under HIPPA[168] and EAR[169] are strict liability, complicated contracting and indemnification clauses are required to apportion liability between cloud providers and consumers (an option unavailable to the general public).

B. The Effect of Generic Laws on Cloud Computing

While there are many regulations weighing upon the cloud computing industry,[170] there is also the standard range of generally applicable laws looming large. Whether companies stand to face a relatively minor penalty under tort principles, as seen in the *Hannaford* case,[171] or the weightier risks Sony faces, remain to be seen.[172] Unless the Sony case is decided in the plaintiff's favor, it appears likely that data breaches may follow the *Hannaford* model, with credit monitoring and fraud restoration providing an easy to calculate and relatively affordable compromise.[173] A ruling for Sony upon the amended complaint seems appropriate, and their offer of "free identity theft protection services, certain free downloads and online services, and '[said that it would] consider' helping customers who [had] been issued new credit cards"[174] would fit well with the *Hannaford* decision. The

167. Breckinridge, *supra* note 96.

168. *See* Jeffrey Roman, *HIPAA Audits: An Update*, HEALTH CARE INFO SEC. (Mar. 22, 2012), http://www.healthcareinfosecurity.com/hipaa-audits-update-a-4607/op-1.

169. *See* Eric R. McClafferty, *Exporting into the Cloud: Export Compliance Issues Associated with Cloud Computing,* INFOTECH SPOTLIGHT (Feb. 2, 2010), http://it.tmcnet.com/topics/it/articles/74329-exporting-into-cloud-export-compliance-issues-associated-with.htm.

170. *See supra* Part III.A.

171. *See* Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162–68 (1st Cir. 2011).

172. It remains to be seen whether the Sony plaintiffs will be able to sufficiently restate a Consolidated Complaint by November 9, 2012. *In re* Sony Gaming Networks and Customer Data Sec. Breach Litigation, Nos. 11cv2119 & 11cv2120, 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012).

173. *See generally* Dian Schaffhauser, *U Hawaii Settles Data Breach Class Action Suit*, CAMPUS TECH. (Jan. 30, 2012), http://campustechnology.com/articles/2012/01/30/u-hawaii-settles-data-breach-class-action-suit.aspx ("The University of Hawaii system has settled a class action lawsuit filed on behalf of 96,000 students, faculty, staff, and alumni who were part of five alleged data breaches at four institutions between 2009 and 2011.").

174. Venkat Balasubramani, *Sony Network Data Breach Class Action Suffers*

prevalence of class-action, tort lawsuits is a symptom of an industry without well-articulated standards and regulations, relying on individual judges' common sense rather than a cohesive set of principles for governing this complex set of technologies and unique problems.

The applicability of the Fourth Amendment provides another platform for litigation. The Supreme Court has refused to reach the issue of whether individuals have a legitimate expectation of privacy in digital communications.[175] A number of lower courts have, however, considered this issue and held that there is a reasonable expectation of privacy in non-local data.[176] Specifically, the nature of modern computing tends to lead to violations of the Fourth Amendment based on overbroad warrants.[177] The Supreme Court's refusal to deal directly with this issue does, however, leave consumers without the ability to predict whether or not their data is open to essentially unlimited searches.

C. Industry Standards and Contractual Issues

In light of the variety of problems service providers face,[178] and the high value of the services they provide,[179] providers often offer what are essentially adhesion contracts in the form of terms of use agreements.[180] In order to manage risk and maximize profit, providers seek to control terms such as when and how data can be accessed, what happens with

Setback – In re Sony Gaming Networks, TECH. & MKTG. LAW BLOG (Oct. 15, 2012), http://blog.ericgoldman.org/archives/2012/10/sony_network_da.htm.

175. City of Ontario v. Quon, 560 U.S. 746, 765 (2010) (holding that the presence of a clause allowing the employer to monitor activity abrogated the need for Fourth Amendment analysis).

176. *See, e.g.*, State v. Bellar, 217 P. 3d 1094, 1107 (Or. App. Ct. 2009) (holding that neither storing data on a hard drive or storing that data in a secure medium owned by a third party destroyed the privacy interest); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *In re* United States' Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d. 1138, 1141 (W.D. Wash. 2011).

177. *In re* United States' Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d at 1144 ("[T]he sheer volume of ESI involved distinguishes a digital search from the search of, for example, a file cabinet.").

178. *See supra* Part I.

179. *See supra* Part II.

180. *See* Mark Taylor, *The Basics of Cloud Computing*, HOGAN LOVELLS, http://ehoganlovells.com/rv/ff0001f56ad18fc97abed201ea4aaf4ecab5ac52/p=1 (last visited Mar. 18, 2014).

that data upon contract termination, what remedies are available, what notice must be given for price changes, flexibility of service provision, and ease of contract termination.[181] Most important from the legal standpoint however, and of greatest importance when negotiations do occur, are clauses dealing with "security, liability and indemnities."[182]

The common primary documents (sometimes combined) in cloud computing contracting are Terms of Services, Service Level Agreements, the Acceptable Use Policy, and the Privacy Policy.[183] Standard service packages include terms that could easily catch users who are unfamiliar with the services off-guard.[184] For instance, in a study of thirty-one terms and conditions packets presented to customers in the United Kingdom, fifteen specified a state in the United States for the choice of law provision.[185] Furthermore, regarding use of the cloud-hosted data, many major providers reserve a great degree of discretion for handling consumer data.[186] One such clause provides for broad discretion for the provider to refuse service, terminate accounts or alter hosted content.[187] Apple's iCloud service also contains a similar clause, giving the provider the discretion to "pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion . . ."[188] Despite the plethora of providers offering completely one-sided terms of service, some do take

181. *See id.*

182. Peter M. Lefkowitz, *Contracting in the Cloud: A Primer*, 54 B. B. J. 9, 10 (2010).

183. Bradshaw et al., *supra* note 148, at 192 (Providing the following definitions: ToS as the document detailing the overall relationship including commercial terms, choice of law, and disclaimers; SLA as a document specifying the level of service the provider will deliver and process for compensation; AUP as permitted and forbidden uses of the service; and Privacy Policy as a document describing the provider's approach to using and protecting customer's personal information including data protection.).

184. *See* Derek Constantine, *Cloud Computing: The Next Great Technological Innovation, The Death of Online Privacy, or Both?,* 28 GA. ST. U. L. REV. 499, 501 (2012).

185. Bradshaw et al., *supra* note 148, at 199.

186. *Id.* at 203.

187. *AWS Site Terms*, AMAZON WEB SERVICES (Dec. 23, 2011), http://aws.amazon.com/terms (stating that, among other things, Amazon "reserves the right to . . . remove or edit content in its sole discretion.").

188. *iCloud Terms and Conditions,* APPLE (Sept. 18, 2013), http:// http://www.apple.com/legal/internet-services/icloud/en/terms.html.

into consideration the needs of their clients.[189] The combination of highly varied terms of service agreements among competitors, frequent unilateral changes to the terms, and the tendency of consumers to forego reading the terms at all, create further problems.[190]

Another major point of concern for consumers, particularly ones subject to privacy regulations such as HIPPA, is the broad range of data disclosure policies.[191] On one hand, some companies require a court order and assist customers in opposing orders to turn over information.[192] On the other side of the spectrum, Facebook is willing to turn over information to "other companies, lawyers, courts or other government entities" in order to "protect ourselves . . ."[193] These terms are not subject to negotiation in the vast majority of cases.

In addition to problems with terms of service and service provision, there are no industry standards for the treatment of data or security measures. A variety of entities including the National Institute of Standards and Technology,[194] the Cloud Security Alliance,[195] and the International Organization for Standardization[196] offer security guidelines, but none of these standards have been uniformly (or even widely) adopted.[197] Although in 2009 several companies such

189. *E.g.*, *AWS Customer Agreement*, AMAZON WEB SERVICES (Mar. 15, 2012), http://aws.amazon.com/agreement ("You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities.").

190. *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: J.L. & POL'Y FOR THE INFO. SOC'Y 540–65 (2008) (analyzing, among other things, how many users actually read privacy policy, to what extent, and at what speed).

191. 42 U.S.C. § 300gg-9(a) (2012).

192. *Master Subscription Agreement*, SALESFORCE ¶ 8.3 (Nov. 27, 2013), https://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf.

193. *How Does Facebook Work with Law Enforcement*, FACEBOOK (Aug. 2013), https://www.facebook.com/help/131535283590645.

194. *Information Technology Portal*, NAT'L INST. OF STANDARDS & TECH (Feb. 13, 2014). http://www.nist.gov/information-technology-portal.cfm.

195. CLOUD SEC. ALLIANCE, https://cloudsecurityalliance.org (last visited Mar. 4, 2014).

196. INT'L ORG. FOR STANDARDIZATION, www.iso.org (last visited Mar. 4, 2014).

197. *See* Christine Lyon & Karin Retzer, *Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud*, CORP. COUNSELOR, Feb. 14, 2011, at 3.

as IBM, CISCO and SAP called for better security and monitoring industry standards in the cloud, Amazon.com, Google, and Microsoft refused to join them.[198] The sheer numbers of purported standards suggest that there is no pending consensus in this area.[199] The lack of these standards increases the importance of contract negotiation and due diligence considering the array of liabilities consumers can be exposed to.

IV. PROPOSAL

The European Union is on the right track with the idea to decrease uncertainty by publishing standards and clearing up the regulatory framework.[200] The danger of this confusion is borne out by the less favorable outlook on cloud computing among United States companies relative to European entities.[201] That Congress is just, as of June 2012, contemplating both the future regulations and the applicability of various existing and potential laws does not bode well for the stability of the cloud computing market. There is a need for quick action or at least clear communication between legislators, the judiciary, prosecutors, and players in the cloud computing industry. This action could come in the form of new legislation, regulations, or a clear choice to abstain from directly regulating cloud computing. What is mandatory, for the potential of cloud computing to be fully realized, is some clear direction given from the entities most capable of destabilizing the industry.

From the standpoint of risk analysis, the content of the recommendation is less important than having direction (regardless of what that direction may be). However, during their inquiries into the demands of data protection in the age of cloud computing, the European Economic Commission

198. David Binning, *Top Five Cloud Computing Security Issues*, COMPUTER WEEKLY (Apr. 24, 2009), http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues.

199. *Welcome To The Cloud Standards Wiki*, CLOUD-STANDARD.ORG (May 13, 2013), http://cloud-standards.org/wiki/index.php?title=Main_Page (last visited Mar. 18, 2014).

200. *See* Ron Tolido, *Cloud Uncertainty is the Enemy of Investment*, FINANCIAL TIMES (Sept. 24, 2012), http://www.ft.com/intl/cms/s/0/fd41369a-fde6-11e1-9901-00144feabdc0.html.

201. *See The State of Adoption of Cloud Applications*, *supra* note 141.

discovered that "economic stakeholders . . . asked for increased legal certainty and harmonization of the rules on the protection of personal data."[202] In line with this sentiment, sure to be similar among U.S. stakeholders, there should be a solitary body of law and clear set of guidelines regarding applicability of other regulations. For instance, rather than having one set of privacy standards under HIPPA (health care information) and another under Payment Card Industry compliance standards (technical and operational requirements that apply to all organizations that process or transmit cardholder data),[203] there should be one uniform set of standards and requirements acceptable for both applications.

A uniform set of laws governing data privacy and security would be beneficial in several respects. For example, service providers' ability to more accurately assess their risk would decrease the need for them to push their risk onto consumers through contracts that force the customer to deal with privacy breaches that are the fault of the provider.[204] While service contract prices may rise in the short term, the focus on price competition rather than competition based on Terms of Service agreements would provide a platform for greater investment and stability over time. Not only would this assist U.S. companies, it would help to lead to further international harmonization and further increase certainty.[205] In addition to consolidating existing federal regulatory schemes, it may be wise for the FTC or another regulatory body to preempt state laws dealing with cloud computing. Although this may not be an entirely popular move, it would

202. European Commission Proposal, *supra* note 62.

203. *See generally* PCI DSS QUICK REFERENCE GUIDE, PCI SEC. STANDARDS COUNCIL (Oct. 2010), https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf.

204. For a discussion of a variety of anti-consumer contractual clauses, *see* David Navetta, *Cyber Insurance: An Efficient Way to Manage Security and Privacy Risk in the Cloud?*, INFO. LAW GRP. (Feb. 1, 2012), http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/cyber-insurance-an-efficient-way-to-manage-security-and-privacy-risk-in-the-cloud/

205. *See* Vineeth Narayanan, Note, *Harnessing the Cloud: International Law Implications of Cloud-Computing*, 12 CHI. J. INT'L L. 783, 808 (2012) ("The second equilibrium state is one in which countries work together, through an agreement or international organization, to design a common set of data protection laws or to minimize jurisdictional clashes by essentially divvying up the 'cloud.'").

prevent these cloud companies from facing a torrent of different standards arising out of individually constructed state consumer protection laws.

CONCLUSION

Participants in the cloud computing market face difficulty both when predicting the future value of present infrastructure and technology investments due to regulatory uncertainty,[206] and when predicting liability costs under the current legal framework. Assuming that many, if not most, managers and directors are at least mildly risk-averse, the perceived cost of participating in the cloud computing market is not close to its optimal value.[207] Current market conditions are suppressed, and future investment in technology is limited because of the risk that any investment in security or certain other types of infrastructure could very easily be incompatible with future regulatory changes.

The surest path towards certainty would be for the United States to follow the lead of the European Union.[208] A unified code system would improve the ability of managers to evaluate their assets, liabilities, and future investments.[209] Although the political economics of regulating major industries is delicate, incremental improvement is mandatory if cloud computing is to reach its full potential.[210] Regardless of whether the U.S. government chooses to regulate heavily or to allow the cloud computing industry to develop in a more unfettered manner, there needs to be clarity and certainty regarding rights, liabilities, and future regulations—conditions glaringly absent at present.

206. *See supra* Part I.D.
207. *See supra* Part II.
208. *See supra* Part IV.
209. *See supra* Part IV.
210. *See supra* Part III.