Journal of Business & Technology Law

Volume 8 | Issue 1 Article 18

Compliance in the Ether: Cloud Computing, Data Security and Business Regulation

J. Nicholas Hoover

J. Nicholas Hoover*

Compliance in the Ether: Cloud Computing, Data Security and Business Regulation

I. Introduction

"To the cloud," Microsoft urged in a recent series of television and Web advertisements.[1] The catchy ads aimed to capitalize on one of the hottest buzz-phrases in the technology industry: cloud computing.[2] "Cloud computing" refers to a new technology paradigm on which businesses and consumers are spending tens of billions of dollars.[3] This paradigm provides users with convenient, on-demand access to a shared pool of computing resources, often over the Internet.[4] Cloud computing offerings like Amazon Web Services provide a professionally managed, nearly unlimited supply of processing power and storage that users can purchase, set up, and access with little more than a mouse click.[5] Businesses increasingly see cloud computing as a valuable proposition for decreasing technology costs,

* J.D. Candidate, May 2013, University of Maryland Francis King Carey School of Law. The author would like to thank his wife for her patience throughout his time in law school and his employer throughout law school, InformationWeek, for providing him with a platform from which to learn about and write about cloud computing and cybersecurity on a regular basis.

1. *See, e.g.*, Windows Videos, *To The Cloud — Start-up — Windows 7*, Dailymotion (Nov. 16, 2010), http://www.dailymotion.com/video/xfnfgp_to-the-cloud-start-up-windows-7_tech.

2. Michael Fitzgerald, *Cloud Computing: So You Don't Have to Stand Still*, N.Y. Times, May 25, 2008, at BU4 ("Cloud computing is the jargon of the moment in the technology industry.").

3. Press Release, Gartner, Inc., Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010 (June 22, 2010), http://www.gartner.com/it/page.jsp?id=1389313.

4. Peter Mell & Thomas Grance, Nat'l Inst. of Standards and Tech., Special Pub. No. 800-145, The NIST Definition of Cloud Computing 2–3 (2011). Such resources may include a variety of services. *Id.* There has been an extensive debate about whether Internet-based access to computing resources is a necessary attribute of cloud computing. *Compare* Andrew Conry Murray, *There's No Such Thing as a Private Cloud*, InformationWeek (Jan. 9, 2009, 3:32 PM), http://www.informationweek.com/cloud-computing/theres-no-such-thing-as-a-private-cloud/229207922 (characterizing the debate as "religious" due to the intransigent position of the sides and arguing that "if you're building all this architecture inside your own data center, and running it yourself, it's not a cloud solution"), *with* Tom Bittman, *Private Cloud Computing Is Real – Get Over It*, Gartner (Feb. 5, 2009), http://blogs.gartner.com/thomas_bittman/2009/02/05/private-cloud-computing-is-real-get-over-it/ (arguing that cloud computing can refer to companies' internal information technology architectures).

5. *About AWS*, Amazon Web Servs., http://aws.amazon.com/what-is-aws/ (last visited Sept. 30, 2012) (touting the cloud computing services' instant deployment benefits)

enabling and accelerating the delivery of new technology services, and refocusing technology workers on mission-oriented tasks that deliver more business value than time spent maintaining corporate technology systems.[6]

And yet, while cloud computing offers numerous advantages, challenges relating to information security, reliability, and compliance with government regulations put users at risk.[7] The CEO of computer networking company Cisco Systems has called cloud computing "a security nightmare."[8] Security and compliance concerns rank among the top barriers to the adoption of cloud computing and present roadblocks to the adoption of cloud services accessed via the Internet.[9] Many businesses remain unprepared for these risks, which if left unaddressed, could expose providers and users to potential liability for regulatory violations and data breaches.[10] This comment principally analyzes public cloud services, as they carry with them the greatest concerns regarding privacy and security.[11]

This comment argues that current laws and regulations governing corporate responsibility for information privacy and security are insufficiently crafted to deal with the shift to cloud computing, and suggests several ways for policy-makers to remedy these legal shortfalls. The comment will first provide readers with an overview of cloud computing and its perceived benefits and disadvantages to businesses and other organizations.[12] It will then analyze how laws and regulatory regimes in financial services, healthcare, and other industries apply to cloud computing, particularly in regards to requirements involving cybersecurity and data privacy.[13] Many of these laws and regulatory regimes have uncertain applicability to cloud computing services since they were passed and implemented prior to the

6. *See infra* Part II.

7. *See infra* Part III.

8. Robert McMillan, *Cloud Computing a 'Security Nightmare,' Says Cisco CEO*, Computerworld (Apr. 21, 2009, 12:00 PM), http://www.computerworld.com/s/article/9131998/Cloud_computing_a_security_nightmare_says_Cisco_CEO.

9. Press Release, North Bridge Venture Partners, 2012 Future of Cloud Computing Survey Exposes Hottest Trends in Cloud Adoption (June 20, 2012), http://www.nbvp.com/2012-future-cloud-computing-survey-exposes-hottest-trends-cloud-adoption (finding that the largest barriers to organizational adoption of cloud computing are security and compliance); *see also* Robert Westervelt, *Cloud Computing Risks Outweigh Benefits, Survey Finds*, SearchCloudSecurity (Apr. 8, 2010), http://searchcloudsecurity.techtarget.com/news/1508319/Cloud-computing-risks-outweigh-benefits-survey-finds (indicating that a survey found that 48% of information technology professionals believe the risks of cloud computing outweigh the benefits, and that regulations obstruct adoption); Harris Interactive Inc., Cloud Computing Final Report 4, 6–7 (2010), *available at* http://www.novell.com/docrep/2010/09/Novell_Cloud_Computing_Survey.PDF (detailing barriers to public cloud adoption).

10. *See infra* Part III.

11. *See* Info. Sys. Audit & Control Assoc., Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives 7 (2009), *available at* http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf (noting concerns about public cloud computing).

12. *See infra* Parts II–III.

13. *See infra* Part IV.

explosion of the cloud computing market and therefore were not drafted with this new technological paradigm in mind.[14] The comment will suggest that federal regulators and other policy-makers take steps to update laws and policy and make a more concerted effort, even if via unofficial guidance, to inform companies how they can be sure that their use of cloud computing services remains compliant with currently applicable regulations.[15]

II. Defining the Cloud

The definition of cloud computing has been subject to much debate, but is slowly taking shape.[16] The term "cloud computing" stems from diagrams of information technology architectures that represent the Internet as a cloud — a distant, undifferentiated patchwork of computing resources.[17] Despite the allusion to a nebulous, ill-defined "cloud" of computing services, however, understanding of the term cloud computing has coalesced sufficiently that the federal government's standards-setting body, the National Institute of Standards and Technology (NIST), has drafted an official definition of its own for use by federal agencies.[18]

NIST defines cloud computing as a computing paradigm that "enabl[es] 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."[19] That means that, among other things, users can access and set up cloud computing services over a network, typically without requiring much additional technical help. [20] In much the same way as buyers of utility services do not have to understand how a power plant generates electricity or a water plant cleans and filters water, cloud computing users typically access cloud computing resources without needing to manage or even understand the underlying computing infrastructure.[21] In many cases, customers pay for access

14. *See, e.g.*, Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2011) (issued in 2002 and made effective in 2003).

15. *See infra* Part V.

16. Jeremy Geelan, *Twenty-One Experts Define Cloud Computing*, Cloud Computing J. (Jan. 24, 2009, 6:15 AM), http://cloudcomputing.sys-con.com/node/612375. One reporter wrote that "nailing down a precise definition of the term is about as easy as grabbing hold of a fluffy cumulus in the sky." Joshua Brockman, *Counting on the Cloud to Drive Computing's Future*, Nat'l Pub. Radio (Mar. 27, 2009), http://www.npr.org/templates/story/story.php?storyId=102453091.

17. Paul T. Jaeger et al., *Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, First Monday (May 4, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171.

18. Mell & Grance, *supra* note 4, at 2.

19. *Id.*

20. *Id.*

21. *See* Info. Sys. Audit & Control Assoc., *supra* note 11, at 4 (2009), *available at* http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf (noting that users are abstracted from the underlying infrastructure on which their cloud computing services operate or store data). In fact, cloud computing has also been referred to as utility computing. Joshua

on a usage basis — per gigabyte, per hour of computing time, or per user.[22] This model contrasts with traditional computing, where an application runs locally on a user's computer or on a single server in a company's data center, where software is bought for a single packaged price or licensed on a long-term basis, and where information technology workers often have to work busily to set up the services and ensure that they are running smoothly.[23]

Cloud computing services are offered in various "deployment models" that are distinguished by how the services are accessed and by whom.[24] Among these models are private, public, and community clouds.[25] Private cloud services and community cloud services, respectively, are for exclusive use by an individual organization or group of organizations and often run inside companies' own data centers.[26] Public cloud services, on the other hand, are broadly accessible by many users and are accessed via the Internet.[27] Public cloud services are available from an array of technology vendors, among them Microsoft, Google, Amazon, and Salesforce.com.[28] These services are typically powered by vast arrays of servers that technology companies house in energy-hungry, warehouse-sized data centers.[29] Public cloud services are often multi-tenant, meaning that one user's data is processed side-by-side with other users' data, rather than being separated by a physical gap between servers.[30] In some cases, applications are widely distributed, meaning that they do not run on any one computer or data center, but perhaps across multiple data centers.[31]

Cloud computing services also come in different service types, which are distinguished by what the cloud service offers. Three different broad categories of

Brockman, *Counting on the Cloud to Drive Computing's Future*, National Public Radio (Mar. 27, 2009), http://www.npr.org/templates/story/story.php?storyId=102453091.

22. Michael Armbrust et al., Univ. of Cal. at Berkeley, Technical Report No. UCB/EECS-2009-28, Above the Clouds: A Berkeley View of Cloud Computing 10 (2009), *available at* http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

23. Chris Weitz, *Cloud Computing and the New Normal*, Network World (Nov. 8, 2010, 12:13 PM), http://www.networkworld.com/news/tech/2010/110810-cloud-computing-new-normal.html.

24. *See* Mell & Grance, *supra* note 4, at 3 (differentiating the deployment models).

25. *Id.*

26. *Id.*

27. *Id.*

28. *Amazon Web Services*, Amazon, http://aws.amazon.com/ (last visited Oct. 3, 2012); *Google Cloud Platform*, Google, https://cloud.google.com (last visited Oct. 3, 2012); *Microsoft on Cloud Computing*, Microsoft News Ctr., http://www.microsoft.com/en-us/news/presskits/cloud/ (last visited Oct. 3, 2012); *What is Cloud Computing?,* Salesforce.com, http://www.salesforce.com/cloudcomputing/ (last visited Oct. 3, 2012).

29. Jaeger et al., *supra* note 17.

30. Wayne Jansen & Timothy Grance, National Institute of Standards and Technology, Special Pub. 800-144, Guidelines on Security and Privacy in Public Cloud Computing 11 (2011) ("[C]lient organizations typically share components and resources with other customers that are unknown to them.").

31. Microsoft, for example, has data centers in Chicago, San Francisco, San Antonio, Dublin, and the state of Washington, among other locations. Ina Fried, *Microsoft's Data Centers Growing By the Truckload*, CNET (Aug. 20, 2008, 9:31 AM), http://news.cnet.com/8301-13860_3-10020902-56.html.

cloud service types exist: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (Iaas).[32] SaaS is equivalent to traditional packaged software that a user might buy or install, and includes services like Microsoft Exchange Online, Google Gmail, and Salesforce CRM.[33] PaaS allows users to build and deploy their own custom applications in the cloud without having to manage or worry about the underlying infrastructure, and includes services like Microsoft Windows Azure and Google App Engine.[34] The IaaS model provides users with a greater level of control over underlying infrastructure and includes services like Amazon Web Services.[35] In the IaaS model, users may have the ability to choose between operating systems, to implement specific network security controls, and to set up their own servers.[36] Public cloud services may offer any of these three service types. In fact, public cloud computing services vary as widely as traditional applications and include services for sharing and storing information, for managing and mining databases, and for hosting Websites and Web services.[37]

III. Cloud Benefits and Pitfalls

A. The Benefits of Cloud Computing

Cloud computing promises numerous potential business benefits. One benefit is that cloud computing accelerates the deployment of technology when compared to traditional information technology architectures, thereby potentially facilitating faster accomplishment of business goals.[38] For example, when the New York Times wanted to make its historic public domain articles more accessible online, the newspaper turned to Amazon's S3 storage and EC2 computing services to generate 11 million article PDFs.[39] This digitization was all accomplished by a single engineer who was able to accomplish the task in less than twenty-four hours for the low cost of $240, a fraction of the time and cost such a project might have required in the world of traditional information technology.[40] It is this type of increased business

32. Mell & Grance, *supra* note 4, at 2–3; *see also* Keith Pijanowski, Understanding Public Clouds: IaaS, PaaS, & SaaS, Keith Pijanowski's Blog (May 31, 2009, 5:40 AM), http://web.archive.org/web/20101101200043/http://www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx. Pijanowski is a Platform Strategy Advisor for Microsoft's Developer and Platform Evangelism Team. *Biography*, KEITHPIJ.COM, http://web.archive.org/web/20101028150638/http://www.keithpij.com/About/tabid/59/Default.aspx (last visited Oct. 3, 2012).

33. Mell & Grance, *supra* note 4, at 2; Pijanowski, *supra* note 32.

34. Mell & Grance, *supra* note 4, at 2–3; Pijanowski, *supra* note 32.

35. Mell & Grance, *supra* note 4, at 3; Pijanowski, *supra* note 32.

36. Mell & Grance, *supra* note 4, at 3; Pijanowski, *supra* note 32.

37. Jaeger et al., *supra* note 17.

38. Info. Sys. Audit & Control Assoc., *supra* note 11, at 6.

39. Derek Gottfrid, *Self-Service, Prorated Supercomputing Fun!*, N.Y. Times Open (Nov. 1, 2007, 5:30 PM), http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/.

40. *Id.*; Bernard Golden, *How Cloud Computing Can Transform Business*, Harvard Bus. Rev. (June 4, 2010, 10:00 AM), http://blogs.hbr.org/cs/2010/06/business_agility_how_cloud_com.html.

flexibility that has led influential business consultancy McKinsey & Company to trumpet cloud computing's "transformational" business possibilities.[41]

Cost savings represent another big draw for cloud computing. Cloud computing may cut companies' information technology costs by twenty percent or more.[42] These savings come from reduced deployment time, limited customization, the self-service nature of cloud services, the lack of up-front costs on technology infrastructure, and often simpler user interfaces that require less training.[43] Additionally, since businesses will only pay for what they need, cloud computing limits what would otherwise be wasted spending.[44]

While decreased costs and increased business flexibility top the list of cloud computing's advantages, there are other benefits. The potential savings and flexibility provided by cloud computing enable companies to take resources that would otherwise be devoted to buying, configuring, and maintaining information technology and refocus them on revenue-driving initiatives.[45] Other miscellaneous benefits as compared to traditional information technology architectures include the abilities to: more easily store large quantities of data; more readily acquire disaster recovery and back-up capabilities; provide access to technologies that users might not otherwise be able to afford; and, in some cases, more effectively and efficiently collaborate.[46]

B. The Security Perils of Cloud Computing

Despite the upside, cloud computing services also raise serious questions about security and privacy.[47] These risks are not all entirely new, as some are analogous to those faced in traditional outsourcing relationships, where companies hand off control of their computing resources to third parties.[48] However, cloud services' complex nature and distributed data architectures make them different from

41. McKinsey & Co., How IT Is Managing New Demands: McKinsey Global Survey Results 1, 7 (2010), *available at* https://www.mckinseyquarterly.com/PDFDownload.aspx?ar=2702.

42. Peter Bisson et al., *The Productivity Imperative*, McKinsey Q., June 2010, at 4, *available at* https://www.mckinseyquarterly.com/PDFDownload.aspx?ar=2630.

43. Abhjit Dubey & Dilip Wagle, *Delivering Software as a Service*, McKinsey Q., May 2007, at 5–6, *available at* https://www.mckinseyquarterly.com/Delivering_software_as_a_service_2006.

44. Info. Sys. Audit & Control Assoc., *supra* note 11, at 6. These cost benefits take on particular significance in times of economic downturn. Andrew R. Hickey, *Cloud Computing, SaaS Boom Fueled By Recession*, CRN (June 22, 2010, 1:48 PM), http://www.crn.com/news/applications-os/225701016/cloud-computing-saas-boom-fueled-by-recession.htm.

45. Jaeger et al., *supra* note 17.

46. Leena Jain & Sushil Bhardwaj, *Enterprise Cloud Computing: Key Considerations for Adoption*, 2 Int'l. J. Eng'g & Info. Tech. 113, 115–16 (2010); World Econ. Forum, Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation 3–4 (2010), http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

47. World Econ. Forum, *supra* note 46, at 9.

48. Info. Sys. Audit & Control Assoc., *supra* note 11, at 7.

traditional outsourcing, causing confusion even as to where data resides.[49] Cloud computing creates an obfuscatory "level of abstraction between the physical infrastructure and the owner of the information being stored and processed" because cloud computing takes control of the physical infrastructure in which data is stored out of the hands of the user, and therefore the user no longer has any natural visibility into operation of that physical infrastructure.[50] This in turn sparks user demand for more transparency regarding service providers' cybersecurity measures, but such assurance may not necessarily be readily provided by cloud providers.[51] The business world's rapid migration from traditional information technology set-ups to cloud computing environments makes these concerns all the more urgent.[52]

Cloud services' distributed, Internet-based nature leaves the services open for attack and may put companies using cloud services at risk of being held legally responsible for losses of information.[53] Public cloud environments are massive, providing hackers with a larger "attack surface" to probe in comparison to private networks.[54] Since public cloud services are delivered online, anyone with Internet access could be a potential hacker.[55] In fact, research indicates that hackers themselves believe that the cloud will open up more hacking opportunities.[56]

Hackers may use a number of pathways to attack the cloud. For example, they may use phishing (seeking information by email or other online channels under false pretenses), fraud, and software exploitation to gain control of users' accounts, giving them the same visibility and control of the cloud service as the users themselves and thus the keys to the kingdom to do as their malevolent hearts

49. *Id.*

50. *Id.* at 4; *see also* Comments of AT&T Before the Department of Commerce Internet Policy Task Force 22 (Jan. 28, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00420-58060.pdf.

51. Cloud vendors have sometimes refused to undergo full compliance audits, as Amazon did when the Internal Revenue Service asked it to help certify EC2 for IRS use, and have expressed a willingness only to do the "bare minimum" to meet legal requirements, as in the case of cloud-based payment processing system Heartland Systems, which was hacked via well-known vulnerabilities in its software. Cloud Sec. Alliance, Top Threats to Cloud Computing 14 (2010), https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf; *see also* Info. Sys. Audit & Control Assoc., *supra* note 11, at 9.

52. Sixty-seven percent of corporate information technology decision-makers believe that there is a rush by U.S. companies and the government "to adopt cloud computing without thinking about the ramifications." Penn, Schoen & Berland Assocs., LLC, Cloud Computing Flash Poll 11 (Jan. 8, 2009), *available at* http://www.doc88.com/p-946596919063.html.

53. Jansen & Grance, *supra* note 30, at 17, 39; *see also infra* Part IV.

54. *Id.* at 12.

55. *Id.* at 11–12.

56. A survey at a 2010 hacker conference found that 96% of attendees believed the cloud would provide them with new avenues of attack, and 45% admitted to already attempting to exploit cloud security holes. Press Release, HP Fortify, DEF CON Survey Reveals Vast Scale of Cloud Hacking – and the Need to Bolster Security to Counter the Problem (Aug. 24, 2010), *available at* http://www.prnewswire.com/news-releases/def-con-survey-reveals-vast-scale-of-cloud-hacking---and-the-need-to-bolster-security-to-counter-the-problem-101361709.html.

desire.[57] Cloud service providers have such a great fear of distributed denial of service attacks, in which attackers flood a website or other online service with so much traffic that back-end systems crash under the traffic's weight, that hackers have been able to extort service providers for tens of thousands of dollars with mere threats of such an attack.[58] Corporate systems interact with and control cloud services via software interfaces known as application programming interfaces, but hackers have attempted to use those interfaces to circumvent policy and potentially expose confidential data.[59] Additionally, researchers have been able to exploit flaws in the technology that aims to separate one customer's data from another and thereby gain control over the underlying physical platforms and affect the operations of multiple customers.[60]

Employee and service provider misuse is also a potential problem. The lack of control and transparency inherent in cloud computing opens up the risk that malicious employees working for the cloud provider could take possession of data to which they should not even have access.[61] Widespread and easy availability of cloud services means that failure (or inability) to control employee use can create risk because employees may bypass the IT department, causing a lack of oversight and placing the company at greater risk in the event of malfeasance.[62] Even something as simple as a configuration error by a cloud service provider could lead to the leaking of sensitive information to unknown actors.[63] Finally, as cloud computing becomes more commonplace, cloud providers themselves may be using other cloud services, leading to potential risks stemming from opaque chains of custody over the data.[64]

57. Cloud Sec. Alliance, *supra* note 51, at 13.

58. Armbrust, *supra* note 22, at 14–15.

59. Cloud Sec. Alliance, *supra* note 51, at 9.

60. *Id.* at 11.

61. *Id* at 10.

62. Jansen & Grance, *supra* note 30, at 14–15. Since business personnel can now bypass the official corporate information technology department and directly sign up for cloud services, formal cloud security policies are thus a necessity for any company. Info. Sys. Audit & Control Assoc., *supra* note 11, at 8.

63. In December 2010, such an error in Microsoft's cloud-based suite of office productivity application exposed customers' corporate data to other customers. Andreas Udo de Haes, *Microsoft BPOS Cloud Service Hit with Data Breach*, Computerworld (Dec. 22, 2010, 11:39 AM), http://www.computerworld.com/s/article/9202078/Microsoft_BPOS_cloud_service_hit_with_data_breach.

64. For example, a social network that relied on other cloud providers to host both historical data and a new database shut down after losing access to customer data, and direct responsibility for the loss was never able to be sorted out. Jansen & Grance, *supra* note 30, at 19–20.

IV. Cloud Computing and Data Security Regulations

Sweeping regulations govern many aspects of corporate life, including how companies must manage and secure their digital data.[65] Data security laws that affect corporate America often address specific industries.[66] These laws include laws and regulations that govern the financial industry, the healthcare industry, and others.[67] However, few laws were written with cloud computing in mind, and in most cases, neither the laws nor accompanying regulations and guidance have been amended to specifically address cloud computing.[68] Some government agencies and officials are beginning to understand the security-related concerns about cloud computing, but are just now beginning to take steps to address those concerns.[69] As a result, compliance is a major concern for cloud service providers and the businesses that use their services.[70] This section will use two example regulations and a survey of other laws to illustrate the clouded application of current regulatory regimes to cloud computing. Specifically, this section will assess how current data security and privacy laws and regulations that govern financial institutions and the healthcare industry should be interpreted in regards to cloud computing, and will survey other regulations that may also need to be looked at differently in regards to cloud computing.

Practitioners can help cut through confusion and concern about cloud computing if they understand how pre-existing law might apply to this new computing model.[71] Increased awareness of how pre-existing law might apply to cloud computing, coupled with increased diligence in adhering to that law, is a must. Information technology professionals remain hesitant to store regulated data such as healthcare data, credit card information, and social security numbers in

65. *See, e.g.*, Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. Tech. L. & Pol'y 229, 238–45 (2011) (detailing various laws that require corporations to secure their data in cloud computing environments).

66. Sunni Yuen, Comment, *Exporting Truth with Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 Colum. Sci. & Tech. L. Rev. 41, 53 n.55 and accompanying text (2008) (describing existing U.S. data protection regulations as "industry or sector-specific").

67. *See, e.g.*, Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2012); OCR HIPAA Security and Privacy Rules, 45 C.F.R. § 164 (2012).

68. Cloud Sec. Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing 45 (v 3.0 2011), *available at* https://cloudsecurityalliance.org/wp-content/uploads/2011/11/csaguide.v3.0.pdf; *see also* Jaeger et al., *supra* note 17 (noting that "few attempts have been made to address the thorny legal issues raised by cloud computing").

69. *See, e.g.*, Letter from Fed. Trade Comm'n Staff to Marlene Dortch, Sec'y, Fed. Commc'ns Comm'n (Dec. 9, 2009), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020352132 (noting that the FTC "is examining 'cloud computing' and its privacy and data security implications for consumers").

70. *See, e.g.*, World Econ. Forum, *supra* note 46, at 9.

71. Cloud Sec. Alliance, *supra* note 68, at 45.

cloud computing environments.[72] However, disconcertingly, compliance practitioners are often at odds with more expert information technology security professionals on their opinion of the level of security of cloud services, with compliance professionals having a more trusting view of cloud services than information security professionals.[73] Furthermore, internal auditors are not often called upon to review cloud security, which exacerbates concerns and confusion through a lack of oversight.[74]

A. Cloud Compliance and Financial Services

The financial industry is heavily regulated.[75] Included among financial regulations are rules requiring companies to keep data secure and private.[76] Failure to follow these regulations has consequences: enforcement actions, including sizable fines, have been levied against financial companies for regulatory non-compliance.[77] Since banks are increasingly adopting cloud services, it is incumbent upon the financial industry to understand how financial industry regulations apply to the use of cloud computing.[78]

Arguably the most important financial industry data security regulation is the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule.[79] GLBA is a comprehensive financial regulation that covers numerous topics, including information privacy.[80] The Safeguards Rule, a regulation promulgated by the Securities and Exchange Commission pursuant to GLBA, sets standards to ensure security and

72. Ponemon Inst. LLC, The Security of Cloud Infrastructure: Survey of U.S. IT and Compliance Practitioners 5 (2011), *available at* http://www.informationweek.com/whitepaper/download/showPDF?articleID=191703837.

73. *Id.* at 1.

74. *Id.* at 11.

75. *See, e.g.*, Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111–203, 124 Stat. 1376 (codified as amended in scattered sections of 2, 5, 7, 8, 12, 13, 15, 18, 22, 26, 28, 31, 42, and 44 U.S.C.).

76. *See, e.g.*, FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1(a) (2012).

77. For example, the Securities and Exchange Commission fined Commonwealth Equity Services, LLP $100,000 for violating a rule requiring brokers and investment advisors to have written policies reasonably designed to safeguard customer information after a hacker stole log-in credentials to a financial system, accessed customer account information, and purchased $523,000 of one publicly-traded company's stock with those accounts. Commonwealth Equity Svcs., LLP, Securities Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929 2–3, 6 (Sept. 29, 2009).

78. Morgan Stanley, for example, has put cloud computing "at the heart of [its] . . . long-term IT strategies." Penny Crosman, *Morgan Stanley Aims for the Clouds*, Wall St. & Tech. (Oct. 19, 2009), http://www.wallstreetandtech.com/articles/220301314; *see also* James Staten, *Are Banks Using Cloud Computing? A Definitive Yes.*, Forrester Blogs (June 1, 2011, 3:27 PM), http://blogs.forrester.com/james_staten/11-06-01-are_banks_using_cloud_computing_a_definitive_yes.

79. 16 C.F.R. § 314.

80. Gramm-Leach-Bliley Act (The Financial Services Modernization Act of 1999), Pub. L. 106–102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.). The information privacy and security sections of the Act, as amended, have been codified in part at 15 U.S.C. §§ 6801–6827 (2011) (regulating disclosure of non-public personal information and fraudulent access to financial information).

confidentiality of customer records and information and protect against threats to and unauthorized access of that information.[81] The Safeguards Rule does not explicitly refer to cloud computing, but it does require oversight of "service provider[s]," defined as entities that receive, maintain, or process customer information through provision of services directly to financial institutions.[82] This definition appears to encompass cloud service providers.

Specifically, the rule requires companies to choose service providers that can appropriately safeguard information and ensure that contractual terms require these safeguards to be maintained.[83] The Safeguards Rule also requires companies to "[i]dentify reasonably foreseeable . . . risks to . . . customer information" and "assess the sufficiency of any safeguards in place to control these risks[,]" which, given cloud computing's clear risks, would include risks of cloud deployments as well.[84]

Overall, the Safeguards Rule is meant to be flexible, requiring only "reasonable steps" to ensure sufficient service provider security.[85] This provides cloud service users leeway as compared to security measures taken in traditional technology set-ups. For example, installing technology to thoroughly monitor information security on a real-time basis may be a reasonable step to take in one's own data center, but may be arduous or impossible in cloud computing scenarios.[86] And while it may sound reasonable for companies to put detailed security requirements into cloud computing contracts, many cloud service contracts are non-negotiable because negotiation of individual contracts may inhibit cloud service providers' economies of scale.[87] However, the Safeguards Rule could be clearer on this point, as it fails to define what "reasonable" means.[88]

In addition to rules related to the Gramm-Leach-Bliley Act, there are other specific restrictions on the types of information financial institutions can share with third parties and how they must go about sharing. For example, laws applicable to

81. 16 C.F.R. § 314.1(a).

82. FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.2(d) (2012).

83. 16 C.F.R. § 314.4(d).

84. 16 C.F.R. § 314.4(b).

85. 16 C.F.R. § 314.4(d)(1).

86. Jansen & Grance, *supra* note 30, at 18 ("Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider.").

87. Rebecca S. Eisner & Daniel Masur, Clear Skies or Stormy Weather for Cloud Computing: Key Issues in Contracting for Cloud Computing Services, Mayer Brown 1 (2010), http://www.mayerbrown.com/public_docs/ARTICLE-Cloud_Computing_Eisner_0910.pdf ("Currently, the standard contracts offered by cloud computing providers are one-sided and service provider-friendly, with little opportunity to change terms."); *see also* Jansen & Grance, *supra* note 30, at 8. *But see* Eric Shoeniger, *Get Your Head in the Cloud*, MoFo Tech + 4 (2010), http://www.mofo.com/files/Uploads/Images/MoFo-Tech-Cloud-2010.pdf ("'There's a perspective that cloud computing is a pre-packaged, one-size-fits-all solution,' [Morrison & Foerster partner Christine] Lyon notes. 'But that's not the case, especially from a privacy and data security perspective.'").

88. 16 C.F.R. § 314.2 (2012).

credit unions, laid out in the National Credit Union Administration Board's Guidelines for Safeguarding Member Information, largely duplicate the terms of the Safeguards Rule[89] but additionally require that credit unions encrypt member information.[90] When individuals obtain financial products for personal or family purposes from financial institutions registered with the Securities and Exchange Commission, those institutions "may not . . . disclose any nonpublic personal information," including account numbers, to "non-affiliated third par[ties]," except under limited preconditions that include allowing consumers to opt out.[91] However, companies may send such information to service providers — and thus store such information in a cloud service — without allowing consumers to opt out of such disclosure, so long as contractual terms prohibit the service provider from improperly disclosing or using the information and, under certain circumstances, so long as notice requirements are met.[92]

It is unclear if federal financial auditors themselves are prepared for cloud computing. The federal government's inter-agency Federal Financial Institutions Examination Council (FFIEC), which is empowered to set standards for federal audits of financial institutions,[93] has created eleven in-depth booklets to help examiners with technology-related audits, including handbooks on e-banking, information security, outsourcing technology services, and supervision of technology service providers.[94] However, while these topics may provide some broad guidance that arguably covers cloud computing, none of the booklets refers to cloud computing in specific terms, and the most applicable booklets have not been updated in years.[95]

Cloud vendors often use claims of compliance with independent, non-government compliance regimes, such as the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements 16 (SSAE16), to prove compliance with official regulatory regimes.[96] For example, Amazon has

89. 12 C.F.R. § 748.0(a), (b)(2) (2012) (requiring each credit union to describe in a written program how it will ameliorate risks); 12 C.F.R. § 748 app. A (III)(B), (D) (requiring identification and assessment of reasonably foreseeable risks and oversight of service providers).

90. 12 C.F.R. § 748 app. A (III)(C)(1)(c).

91. 17 C.F.R. § 248.1, .10, .12 (2012).

92. 17 C.F.R. § 248.13(a), .14.

93. 12 U.S.C. §3305(a) (2011).

94. *IT Booklets*, FFIEC Examination HandBook InfoBase, http://ithandbook.ffiec.gov/it-booklets.aspx (last visited Oct. 6, 2012).

95. A handbook on supervision of technology service providers, for example, has not been updated since March 2003 — eons in the technology world. Fed. Fin. Insts. Examination Council, Supervision of Technology Service Providers IT Examination Handbook 1 (2003), *available at* http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders.pdf.

96. For further details on the SSAE16 assessment, see American Institute of Certified Public Accountants, Reporting on Controls at a Service Organization (2011), *available at* http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf. This standard replaces the popular Statement on Auditing Standards No. 70 (SAS 70), which was used for the same purpose.

stated that its SSAE16 compliance report, which includes details on user account access controls, logical and physical security controls, safeguards against malfunctions and physical disasters, and data integrity efforts, should assure customers of compliance with "a broad range of financial auditing requirements."[97] In the traditional technology world where companies own and host their own systems and services, companies themselves can audit their own systems or hire a third party to do so for them. However, while Amazon will send users summary reports of its audits, cloud service users simply have to take Amazon at its word, since Amazon does not allow users in its data centers to directly assess Amazon's controls.[98] This is one of the major obstacles to cloud compliance: users are not able to independently audit cloud service providers' IT infrastructures, but must instead rely on the service providers to perform such audits.[99]

B. Healthcare in the Cloud

Organizations that possess personal healthcare information must comply with the Health Insurance Portability and Accountability Act (HIPAA), as modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act.[100] Regulations accompanying these laws require regulated entities to take certain steps to ensure data security and confidentiality.[101] Failure to comply can be costly: the maximum possible fine for a violation is $1.5 million, and there is a possibility of civil penalties even for unknowing violations.[102] Furthermore, there is a prospect of more widespread punishment, as the Department of Health and Human Services' Office for Civil Rights has plans for a permanent, official HIPAA

Press Release, Am. Inst. of Certified Pub. Accountants, AICPA Publishes New Attest Guidance for Reporting on Controls at a Service Organization (June 29, 2011), *available at* http://www.aicpa.org/press/pressreleases/2011/pages/aicpapublishesnewattestguidanceforreportingoncontrolsataserviceorganization.aspx.

97. Amazon Web Servs., Amazon Web Services: Risk And Compliance 4, 6–7 (2011), *available at* http://d36cz9buwru1tt.cloudfront.net/AWS_Risk_and_Compliance_Whitepaper.pdf.

98. *Id.* at 10.

99. Sara Peters, *Can Businesses Prove Compliance in the Cloud?*, Wall St. & Tech. (Dec. 6, 2008), http://www.wallstreetandtech.com/articles/212700784. Additionally, such audits may be insufficient alone to assure security or compliance, as they may be only "high-level" reviews. *Id.* This represents a potential conflict of interest heightened by a lack of transparency.

100. Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d (2011) (includes the privacy and security sections of HIPAA); Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 17931–40 (2011). Other regulations on the use of patient information, such as those on the confidentiality of alcohol and drug abuse patient records, may also apply to such organizations, but are beyond the scope of this comment. *See, e.g.*, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. pt. 2 (2012).

101. 45 C.F.R. pt. 164 (2012).

102. 45 C.F.R. § 160.404 (2012).

audit program.[103] With some covered organizations moving data to the cloud, it is imperative that they understand how HIPAA applies to cloud computing.[104]

HIPAA regulations have many data security requirements.[105] Generally, they command healthcare organizations and organizations that possess healthcare data to "ensure the confidentiality, integrity, and availability" of personally identifiable healthcare data, and to protect against threats to and unauthorized use or disclosure of that data.[106] Regulations enable a flexible approach to meeting these requirements.[107] However, they require organizations to take a number of specific measures, including risk analysis, regular reviews of information security, action in response to suspected or known security incidents, and the assignment of unique user names.[108]

While some HIPAA safeguards are required, others are labeled as "addressable," meaning that they should be implemented if reasonable and appropriate.[109] These include encryption of protected healthcare information and policies for authorizing access to protected healthcare information.[110] While making these safeguards optional provides covered entities with an additional degree of flexibility, some of these security measures may in fact be reasonable and appropriate when storing private data in an Internet-accessible cloud computing service, and companies must, therefore, make a conscious choice about how to secure their cloud services.[111] For example, healthcare claims management company TC3 Health, which has access to sensitive health records, encrypted all of its data before moving it to the cloud in order to maintain HIPAA compliance.[112]

Companies must think about HIPAA compliance when contracting for cloud computing services. It is not enough to take the word of cloud providers like Amazon that claim that their cloud computing infrastructures are or can be HIPAA-compliant.[113] While HIPAA regulations do not explicitly refer to cloud computing, contracts between entities covered under HIPAA and their "business

103. Howard Anderson, *Permanent HIPAA Audit Program Coming*, GovInfo Security (Nov. 17, 2011), http://www.govinfosecurity.com/articles.php?art_id=4253.

104. Microsoft offers a number of case studies on healthcare companies that have moved email, collaboration, and other services to Microsoft data centers. *Cloud Services for Health*, Microsoft, http://www.microsoft.com/health/en-us/initiatives/Pages/cloud-services-for-health.aspx (last visited Oct. 6, 2012).

105. 45 C.F.R. pt. 164.

106. 45 C.F.R. § 164.306(a) (2012).

107. *See, e.g.*, 45 C.F.R. § 164.306(b)(1) (2012) (allowing covered entities to use "any security measures that allow the covered entity to reasonably and appropriately implement the standards").

108. 45 C.F.R. §§ 164.308–312.

109. 45 C.F.R. § 164.306(d)(3).

110. 45 C.F.R. § 164.308(a)(4)(ii)(B), 164.312(a)(2)(iv).

111. Remember, after all, the security risks posed by the cloud. *See supra* Part III.

112. Armbrust, *supra* note 22, at 15.

113. *E.g.*, Amazon Web Servs., *supra* note 97, at 9 ("The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA.").

associates" must provide for the implementation of security capabilities that "reasonably and appropriately" protect health information.[114] Many cloud service providers would most likely be considered to be "business associates" under the regulatory definition of the term — which, in short, includes any service provider that performs or facilitates the use or disclosure of individually identifiable health information — and therefore might often be said to be subject to HIPAA.[115] Covered entities may remain liable for non-compliance with these requirements even if their data is hosted with a cloud service provider.[116] For example, when wound therapy company GWR Medical, Inc. moved its technology operations to Verizon Business' cloud computing infrastructure, the two parties hammered out contractual language specific to HIPAA.[117]

Unfortunately, cloud computing contracts are sometimes non-negotiable, standard business associate agreements are far from ubiquitous, and even having a business associate agreement in place is insufficient standing alone to ensure compliance.[118] Contracts for Microsoft's HealthVault service include a standard "business associate agreement" obligating Microsoft to use "appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as permitted," report unauthorized disclosures, and create additional agreements with subcontractors that might have access to data.[119] However, even at large companies like Microsoft, these contractual terms have only recently begun to become

114. 45 C.F.R. § 164.314(a)(2)(i) (2012).

115. *See* 45 C.F.R. § 160.103 (2012) (defining, among other terms, "business associate"). In particular, vendors that host "software containing patient information" on their own servers, as cloud service providers may do, should be considered business associates. *Is a Software Vendor a Business Associate of a Covered Entity?*, Dep't. of Health & Human Servs. (Mar. 14, 2006), http://www.hhs.gov/hipaafaq/providers/business/256.html. *But see* Robert Gellman, World Privacy Forum, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing 9 fn. 9 (2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (concluding that under some circumstances cloud service providers might not be considered business associates).

116. Ed Moyle, *Why Cloud Computing Changes the Game for HIPAA Security*, TechNewsWorld (Apr. 19, 2011, 5:00 AM), http://www.technewsworld.com/rsstory/72291.html (noting that "[u]ltimate responsibility for compliance always resides at the covered entity").

117. Marcia Savage, *HIPAA Business Associate Agreement Key to Company's Cloud Migration*, SearchCloudSecurity.com (Feb. 8, 2011), http://searchcloudsecurity.techtarget.com/news/2240031913/HIPAA-business-associate-agreement-key-to-companys-cloud-migration.

118. Joshua J. Freemire & James B. Wireland, Ober | Kaler, *HIPAA Considerations in Evaluating Cloud Computing*, Health L. Alert Newsl. (2012), http://www.ober.com/publications/1645-hipaa-considerations-evaluating-cloud-computing ("By its very nature, the multi-tenant environment that characterizes the public cloud involves a certain 'lowest common denominator' with respect to system features like encryption. Not all vendors are willing to deploy encryption if most of their users do not require it."). This argument holds true despite the fact that recently issued regulations clarify that business associates must meet certain HIPAA privacy requirements. *See* 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013).

119. *HealthVault Business Associate Agreement*, Microsoft, *available at* http://download.microsoft.com/download/7/1/9/719944BB-2A59-428D-B220-EB50DA188850/HealthVault%20HIPAA%20Business%20Association%20Agreement.docx (last visited Oct. 5, 2012).

standardized.[120] Furthermore, even if a business associate agreement is in place, organizations covered by HIPAA will fall out of compliance if they fail to take steps to cure known breaches of the agreement.[121]

C. Other Compliance Regimes

While financial and healthcare regulations are arguably the most comprehensive and widely applicable of the regulations that likely apply to cloud computing, a dizzying array of other regulations also require new interpretation of privacy and security compliance. One well-known provision, Section 404 of the Sarbanes-Oxley Act, requires public companies to attest to the effectiveness of their internal controls for financial reporting, which include controls on the information systems that manage the data that serves as a basis for those reports.[122] Audit standards promulgated by the Sarbanes-Oxley-created Public Company Accounting Oversight Board require assessment of information technology controls.[123] However, Sarbanes-Oxley is by no means the only other regulation for which the arrival of cloud computing could have consequences.

Numerous regulations and guidance documents require organizations to "conduct extensive due diligence" on service providers and monitor their compliance.[124] Federal contractors must afford government access to their facilities to safeguard against data security threats, but regulations are silent on whether such requirements also fall to those contractors' subcontractors.[125] Massachusetts has state-specific data security regulations with a service provider provision.[126] The Stored Communications Act limits the circumstances under which certain service providers may disclose customer data and creates a right to sue violators.[127]

120. For example, as of the summer of 2011, Microsoft was still working on business associate agreements for some of its more popular cloud services. John Spilker, Microsoft, *Understanding and Differentiating Microsoft's Approach to Governance, Risk and Compliance in Health*, Microsoft Health Users Group (July 1, 2011, 8:02 PM), http://mshug.org/b/webinars/archive/2011/07/01/understanding-and-differentiating-microsoft-s-approach-to-governance-risk-and-compliance-in-health.aspx.

121. 45 C.F.R. § 164.504(e)(1)(ii) (2012).

122. Sarbanes-Oxley Act, 15 U.S.C. § 7262 (2011), *amended by* Jumpstart Our Business Startups Act, Pub. L. No. 112–106, 126 Stat. 310 (2012).

123. Pub. Co. Accounting Oversight Bd., Auditing Standard No. 5, Release No. 2007-005A A1-14, 18, 22, A4-12–13 (2007).

124. Joseph I. Rosenbaum & Leonard A. Bernstein, Reed Smith, *Look, Up in the Cloud . . . It's a Bird, It's a Plane, It's a Bank*, *in* Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing 36, 37 (Joseph I. Rosenbaum ed., 2010), http://www.reedsmith.com/files/Publication/c3ff697f-fe78-47b8-af1c-88068c8481a0/Presentation/PublicationAttachment/d40d7c3b-9fac-4882-8cb8-8eddb9331527/78282026_1.pdf.

125. 48 C.F.R. § 52.239-1(b) (2012).

126. 201 Mass. Code Regs. 17.03(f) (2009).

127. Stored Communications Act, 18 U.S.C. §§ 2702, 2707 (2011).

However, its terminology, like that of many other laws and regulations, may be outdated in the cloud era.[128]

V. The Way Forward for Cloud Compliance

The guesswork required to shoehorn cloud computing into years-old compliance regimes, even combined with industry self-regulation, is an inefficient and uncertain way to deal with such a revolutionary new technology. As more and more consumer and enterprise data moves into cloud computing environments, increasing uncertainty about legal and regulatory obligations could jeopardize or slow the adoption of cloud computing and thereby hinder the aggregate business benefits that cloud computing could bring to the broader economy.[129] Policy-makers must do a better job at communicating the applicability of compliance regimes to emerging cloud computing services, whether by new or updated legislation and regulation, or even by promulgating unofficial guidance.[130] There are numerous workable solutions to this problem, but any fix must be consistent and clear and must balance the various stakeholders' interests and needs.

There are some general best practices that apply to cloud computing, and government can better align regulations with those best practices.[131] Policy-makers need not draw from a blank regulatory slate, as the government and private sector are already working in some spheres to provide detailed guidance for cloud compliance. The credit card industry, for example, has written cloud computing guidance for its own Payment Card Industry Data Security Standard.[132] One non-profit organization with support from major cloud vendors, CloudAudit, has created a matrix matching up suggested security controls with their supposed regulatory bases in various compliance regimes.[133] Additionally, the federal

128. Timothy Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. Pat. & Trademark Off. Soc'y 283, 306–07 (2010). *But see* J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform* 5 n.15 (2010), *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf ("We interpret the current definition of remote computing service as broad enough that it does not need to be amended to cover technologies such as cloud computing.").

129. Microsoft, Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing 2 (2010), *available at* http://download.microsoft.com/download/C/0/0/C00D24A5-A686-4109-9DB8-14A29E058069/Building_Confidence_in_the_Cloud_White_Paper.doc ("The private sector . . . cannot build user confidence in the cloud on its own. The solution requires a cooperative effort from all stakeholders, including governments.").

130. *See* World Econ. Forum, *supra* note 46, at 9 (highlighting compliance concerns as among the "biggest barriers" to cloud computing adoption). Other commentators have also bemoaned legal uncertainty and unpredictability in the cloud and suggest a legislative response. *See, e.g.*, Gellman, *supra* note 116, at 7–8.

131. *See* World Econ. Forum, *supra* note 46, at 9 (recommending that governments create clear rules on privacy, data ownership, and liability vis-à-vis cloud computing).

132. PCI Sec. Standards Council, Information Supplement: PCI DSS Virtualization Guidelines 22–24 (2011), *available at* https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

133. *Cloud Controls Matrix*, Cloud Sec. Alliance (2012), *available at* https://cloudsecurityalliance.org/research/ccm/.

government has set up a "standardized approach to the security authorization process for cloud products and services" including a list of more than 300 recommended and required security controls, that ensures that cloud services meet the requirements of the Federal Information Security Management Act, the law that governs data security for federal agencies.[134]

Regulatory changes could help mitigate cloud users' lack of insight into and control over their providers' cloud computing environments. Policymakers should, for example, encourage cloud computing providers to be more transparent with their data practices, such as by informing customers whether the cloud provider will hold onto data after the user terminates its relationship with the cloud provider, and how that data will be used.[135] Such a move could help companies understand their compliance footing by enabling them to better assess risks to privacy and confidentiality.[136] Service providers may be willing to sign on to such a law: Microsoft itself has suggested such legislative change.[137] Regulators could additionally set policy to encourage negotiable terms in cloud computing contracts, which also may open the room for more dialogue on security measures.[138]

The rise of cloud computing may also present a perfect opportunity to begin to unify the disparate data security compliance regimes, which overlap in many ways but are inconsistent in other ways. The cloud computing industry itself seeks a more unified approach to cloud compliance, viewing government regulations as complex and inconsistent.[139] More than half of the respondents to a recent World Economic Forum survey agreed, saying that governments should reduce the complexity of compliance requirements and establish across-the-board cloud security standards to help accelerate adoption of cloud computing.[140] Several bills recently introduced in Congress could have blanket application to all companies that handle personal and other private data, such as the Personal Data and Breach Accountability Act of 2011, but these acts largely fail to specifically address cloud computing, and, rather than decreasing the reporting burden by eliminating other regimes, might instead just layer on additional or duplicative requirements.[141]

134. Richard Spires, Chief Information Officer, Dep't of Homeland Sec., *FedRAMP Security Requirements Benchmark IT Reform*, CIO.GOV (Jan. 6, 2012), https://cio.gov/fedramp-security-requirements-benchmark-it-reform/; *see also* GEN. SERVS. ADMIN., FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP) SECURITY CONTROLS (2012), http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls.zip.

135. *See* Comments of AT&T, *supra* note 50, at 22 (recommending such laws).

136. *See* GELLMAN, *supra* note 115, at 7–8 (bemoaning the lack of certainty in compliance regimes that apply to cloud computing).

137. MICROSOFT, *supra* note 129, at 6–7.

138. *See supra* text accompanying note 86.

139. WORLD ECON. FORUM, *supra* note 46, at 11.

140. *Id.* at 14.

141. *See, e.g.*, CONG. BUDGET OFFICE, COST ESTIMATE: PERSONAL DATA PROTECTION AND BREACH ACCOUNTABILITY ACT OF 2011 4–5 (2011), *available at* http://www.cbo.gov/ftpdocs/125xx/doc12563/s1535.pdf.

Congress could also provide for additional punishments for those convicted of hacking, which may decrease the threat of attack and thus the threat of liability on the part of regulated companies.[142] Microsoft has suggested the Congress amend the Computer Fraud and Abuse Act to make it easier to impose felony penalties on hackers, increase the maximum fine to $250,000 per account illegally accessed, and give cloud service providers themselves a private right of action against hackers.[143] Policy-makers may also want to make a push to prevent or at least limit the disclaimer of cloud providers' own liability, which may encourage providers to adopt stronger security measures and help to distribute the privacy and security burden more equally among hackers, service providers, and regulated entities.[144]

VI. Conclusion

There is still time to act before the cloud revolution passes regulators by, but the sooner regulators begin to act, the better off regulated businesses will be.[145] Cloud computing is a popular and potentially transformative technology.[146] However, few of the many regulations that govern broad aspects of American corporate life have been updated to address the unique concerns about data privacy and security implicated by cloud computing.[147] This leaves businesses with little choice but to resort to guesswork in their understanding of how regulations apply to their use of cloud computing services.[148] Policy-makers can and must clarify the law as it applies to cloud computing.

142. Allan A. Friedman & Darrell M. West, *Privacy and Security in Cloud Computing*, Issues in Tech. Innovation 8 (Oct. 2010), http://www.brookings.edu/~/media/Files/rc/papers/2010/1026_cloud_computing_friedman_west/1026_cloud_computing_friedman_west.pdf.

143. Microsoft, *supra* note 129, at 5.

144. Rebecca S. Eisner & Daniel Masur, *Clear Skies or Stormy Weather for Cloud Computing: Key Issues in Contracting for Cloud Computing Services*, Mayer Brown (Sept. 2010), http://www.mayerbrown.com/public_docs/ARTICLE-Cloud_Computing_Eisner_0910.pdf ("Many [cloud computing contracts] . . . disclaim all or most of the provider's potential liability.").

145. Alistair Maughan et al., Morrison & Foerster, Global Sourcing Trends in 2011 5 (2011), http://www.mofo.com/files/Uploads/Images/110118-Global-Sourcing-Trends.pdf (predicting that regulators will be slow to create regulations that provide guidance to regulated industries, and that cloud adoption in those industries will lag as a result).

146. *See supra* Parts I–III.

147. *See supra* Part IV.

148. *See supra* Part IV.