HEAD OUT OF THE CLOUDS: WHAT THE UNITED STATES MAY LEARN FROM THE EUROPEAN UNION'S TREATMENT OF DATA IN THE CLOUD

Jenna Gerber*

I. INTRODUCTION

"Every cloud has its silver lining but it is sometimes a little difficult to get it to the mint."[1]

An attorney is awakened at 3:00 a.m. by a phone call from police. There has been a break-in at his firm, and a laptop filled with hundreds of client files containing sensitive data of payment records, client addresses and phone numbers, and trial strategies was stolen. Fortunately, the attorney has back-up files, knows what is missing, and who potentially has been affected. Later that morning, the hundreds of clients who have sought confidential advice from that attorney are alerted that their information has been stolen. It is a nightmare for many of the firm's attorneys, but the physical evidence immediately alerted the staff that there had been a security breach, and the office was able to respond to the situation quickly and effectively. The attorney decides that the solution to preventing the risk of having sensitive data stolen off the hardware from the office is to move all client data "to the cloud." Only those with authority would be able to access the data on the remote server, so even if a laptop were to go missing, nothing would be compromised. The problem, though, is that there may not be the same physical evidence of a breach, and an attorney or client may never know of a security threat because the information is stored on a remote server. The paradox of moving to the cloud is that personal data is, in many ways, more secure and less secure than it has ever been.

Cloud computing has been growing in size and momentum in informational technology's collective conscience ever since the phrase was first used in its current context in 1997.[2] The concept itself, though, is not really new, dating back at least to the 1960s.[3] The name derived from telecommunication companies who changed their services from point-to-point circuits to Virtual Private Networks in the 1990s, and subsequently

---

* Jenna Gerber is a 2013 J.D. candidate at the Indiana University Robert H. McKinney School of Law.

1. Don Marquis, *available at* http://quotationsbook.com/quote/10933/.

2. Sourya Biswas, *A History of Cloud Computing*, CLOUD TWEAKS (Feb. 9, 2011 6:40 AM), http://www.cloudtweaks.com/2011/02/a-history-of-cloud-computing/ (Ramnath Chellappa defined cloud computing as a new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone.").

3. *Id.*

the Internet was visualized as diagrams of clouds in textbooks.[4] Thus, the phrase "cloud computing" was born. Still, cloud computing is quite undefined for many common users of the Internet, nothing more than a buzzword and a vague concept.[5] Others emphasize that cloud computing is a "buzzword almost designed to be vague, but. . .is more than just a lot of fog."[6] The National Institute of Standards and Technology (NIST) defines cloud computing as:

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[7]

In layman's terms, cloud computing allows users (be it an individual or a multi-national corporation) to gain access to resources, such as remote hosting and storage, so the burden is off the user to provide an infrastructure or support for such an infrastructure. The infrastructure is hosted at a remote location and can be shared by multiple users to increase efficiency.[8] Though marketing campaigns advertise "the cloud" as a seemingly singular entity,[9] cloud networks are diverse in size, shape, and complexity, and more are created each day. For the attorney in the example above, instead of having to pay thousands of dollars to purchase and maintain an internal server for the firm, a simple move to the cloud[10] would increase storage and efficiency while decreasing costs and reducing the need for extensive internal IT support and maintenance.

This Note will first explain cloud computing on a basic level and highlight the challenges in regulating overseas transmission of data from both a technological and legal standpoint. Second, this Note will examine the current and proposed legislation in the United States that regulate the

---

4. *Id.*

5. PHILIP KOEHLER ET AL., CLOUD SERVICES FROM A CONSUMER PERSPECTIVE 2 (2010) *available at* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.174.6121.

6. *Id.*

7. PETER MELL & TIMOTHY GRANCE, NAT'L. INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (Sept. 2011), *available at* csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [hereinafter NIST].

8. *The Benefits of Cloud Computing*, DELL, http://content.dell.com/us/en/enterprise/cloud-computing-value-benefits (last visited Oct. 6, 2012).

9. For specific examples, see a selection of Microsoft's Windows 7 commercials with the tag line "to the cloud,. "Family Photo" – To the Cloud – Windows 7, Microsoft Windows (last visited Nov. 25, 2012), *available at* http://www.youtube.com/watch?v=mjtqoQE_ezA.

10. For purposes of this Note, when "the cloud" is mentioned, it refers to a cloud computing infrastructure generally, and not a specific product or nebulous public cloud.

cloud and significant cases that render most current law inapplicable. Third, this Note will engage in a comparative analysis of the European Union's current legislation and pending changes compared to policy in the United States. Finally, this Note will argue that the United States should move quickly to enact legislation regulating the use of the cloud before it becomes too late, and adopt several policies already in place in the European Union to protect user privacy stateside.

II. CLOUD COMPUTING BASICS

A. The Three Service Model Types of Cloud Computing

Clouds take on many different forms and functions depending on the needs of the end users, the provider's framework, and the goal of the service exchange.[11] The three service models upon which clouds are built are Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service.[12]

Among the first cloud computing services offered to the public was Webmail, an Internet-based interface that offered email services.[13] The consumer embrace of such technology led to "rapid development of other cloud-based applications, including calendars, contact management, word processing, and digital photo applications."[14]These types of services, known as Software-as-a-Service (SaaS) or "on-demand software," have been heralded as the model that reduces costs considerably and simplifies technical support and maintenance.[15] Payment for SaaS is flexible, as it may be billed by usage, on a subscription basis, or free if advertisements cover the cost.[16] Some, however, are critical of SaaS and encourage users to beware of buying into the hype.[17] The NIST defines SaaS as:

---

11. *See generally* THE FUTURE OF CLOUD COMPUTING: OPPORTUNITIES FOR EUROPEAN CLOUD COMPUTING BEYOND, EUROPEAN COMMISSION ON INFORMATION SOCIETY AND MEDIA (Keith Jeffery & Burkhard Neidecker-Lutz eds., 2010), *available at* http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (last visited Oct. 6, 2012).

12. *Id.* at 9-10.

13. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1203 (April 2010).

14. *Id.*

15. Steve Lohr, *Wal-Mart Plans to Market Digital Health Records System*, N.Y. TIMES (Mar. 10, 2009), http://www.nytimes.com/2009/03/11/business/11record.html.

16. Sourya Biswas, *Cloud Computing for Dummies: SaaS, PaaS, IaaS, and All That Was*, CLOUDTWEAKS (Mar. 20, 2012), http://www.cloudtweaks.com/2011/02/cloud-computing-for-dummies-saas-paas-iaas-and-all-that-was/.

17. *See generally* Galen Gruman, *The Truth about Software as a Service (SaaS)*, CIO (May 21, 2007), http://www.cio.com/article/109706/The_Truth_About_Software_as_a_Service_SaaS_?page=3&taxonomyId=3000; Gene Marks, *Beware the Hype for Software as a Service*, BLOOMBERG BUSINESSWEEK (July 24, 2008), http://www.businessweek.com/technology/content/jul2008/tc20080723_506811.htm.

> The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[18]

Popular forms of these services attract millions of unique users each month, such as Facebook (2,569,233 unique visitors per month),[19] Twitter (2,446,305 unique visitors per month),[20] Yahoo! Mail (445,539 unique visitors per month),[21] and Shutterfly (258,907 unique visitors per month).[22] Despite the popularity of SaaS frameworks, "[m]any providers are shifting away from designing their own applications. . .and instead [are] opening up their systems to third-party developers who create applications that run on the cloud provider's platform."[23] Some are dissatisfied with SaaS providers because "they might allow you to export your data, but they usually [do not] allow you to export their underlying code. . ..[T]hey have a lot more in common with proprietary software vendors than Open Source projects or companies."[24]

The second model, Platform-as-a-Service (PaaS), allows programmers the flexibility to combine the capabilities of multiple cloud applications into one.[25] Users have "limited control over the software so long as it does not interfere with the physical infrastructure of the provider's network."[26] NIST defines PaaS as:

---

18. NIST, *supra* note 7.

19. Facebook Statistics, SITEANALYTICS.COMPLETE.COM (Mar. 20, 2012), http://siteanalytics.compete.com/facebook.com/October2011Data.

20. Twitter Statistics, SITEANALYTICS.COMPLETE.COM (Mar. 20, 2012), http://siteanalytics.compete.com/twitter.com/October2011Data.

21. Yahoo! Mail Statistics, SITEANALYTICS.COMPLETE.COM, (Mar. 20, 2012), http://siteanalytics.compete.com/mail.yahoo.com/October2011Data.

22. Shutterfly Statistics, SITEANALYTICS.COMPLETE.COM (Mar. 20, 2012), http://siteanalytics.compete.com/shutterfly.com/October2011Data.

23. Robison, *supra* note 13, at 1203.

24. Alex Williams, *Drupal Founder Critical of SaaS and its Proprietary Nature*, READWRITEWEB/ ENTERPRISE (Mar. 2, 2010), http://www.readwriteweb.com/enterprise/2010/03/drupas-founder-says-the-saas-m.php.

25. Robison, *supra* note 13.

26. Shahid Khan, *"Apps.gov": Assessing Privacy in the Cloud Computing Era*, 11 N.C. J.L. & Tech. On. 259, 266 (2010).

> The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.[27]

PaaS infrastructures are rarer for the common user to interact with, but popular examples are Google's App Engine, Microsoft's Azure, and Salesforce.com's Force.com.[28] Salesforce.com advocates the use of PaaS because it "provides all the infrastructure needed to run applications over the Internet."[29] Additionally, PaaS works as a utility; users "tap in" and use only what they need, no more, no less, and the service is delivered without the consumer having to worry about what is going on behind the scenes.[30] Also, like a utility, PaaS consumers simply pay for what they use based on a metering rate.[31]

The third type of service model available for cloud users is an Infrastructure-as-a-Service (IaaS), or Hardware-as-a-Service, model. Using IaaS, cloud providers sell data storage, processing power, and other raw computer resources.[32] The consumer decides the type of operating system and how to allocate resources, though the provider controls the physical network.[33] NIST defines IaaS as:

> The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select

27. NIST, *supra* note 7.

28. Biswas, *supra* note 16.

29. *What Is Platform as a Service*, SALESFORCE.COM, http://www.salesforce.com/paas/ (last visited Jan. 2, 2013).

30. *Id.*

31. *Id.*

32. Robison, *supra* note 13, at 1204.

33. Khan, *supra* note 26, at 266.

networking components (e.g., host firewalls).[34]

Perhaps the most successful and most pervasive form of an IaaS is Amazon's Elasic Compute Cloud (Amazon EC2). Amazon advertises EC2 as being able to "provide[] . . . complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change."[35]

Each service model provides varying levels of flexibility and control for the user and different benefits may be derived from each, depending on unique needs.[36]

B. Four Deployment Models of the Cloud

While many of the common users may not have an interest in what type of service-model is used, one privacy aspect that users may want to take note of is the deployment model their cloud is using. The four models – the private cloud, the community cloud, the public cloud, and the hybrid cloud – offer varying access and privacy to users.[37]

The private cloud is structured for the smallest group of users, as its infrastructure is used by one organization with multiple consumers.[38] "Strictly speaking such infrastructure does not form part of the cloud and the 'private cloud' is really a description of a highly virtualized, local data centre that is behaving as if it was delivered by a public cloud provider."[39] Private clouds offer more control over access to data and the physical location of the servers but may come at a higher cost.[40] Critics are skeptical of this model, however, because "IT departments still have to buy, build, and manage them" which goes against the premise of hands-off maintenance,[41] and private clouds "lack[] the economic model that makes cloud computing such an intriguing concept in the first place."[42]

A community cloud is an infrastructure that allows a community of

34. NIST, *supra* note 7.

35. *Amazon Elastic Compute Cloud,* AMAZON.COM, http://aws.amazon.com/ec2/ (last visited Mar. 20, 2012).

36. *See* THE FUTURE OF CLOUD COMPUTING, *supra* note 11, at 10-11.

37. NIST, *supra* note 7.

38. *Id.*

39. *Cloud Deployment Models,* JISC INFONET, http://www.jiscinfonet.ac.uk/infokits/cloud-computing/deployment-models (last visited Jan. 2, 2013).

40. *Id.*

41. John Foley, *Private Clouds Take Shape,* INFORMATIONWEEK (Aug. 9, 2008, 12:00 AM), http://www.informationweek.com/news/services/business/209904474.

42. Gordon Haff, *Just Don't Call Them Private Clouds,* CNET (Jan. 27, 2009 9:12 AM), http://news.cnet.com/8301-13556_3-10150841-61.html.

organizations to share cloud space while striving for similar objectives, such as common security requirements or compliance obligations.[43] The organizations themselves may manage the infrastructure, or the task may be assumed by a third party.[44] The United States government, for instance, uses a community cloud that is managed by Google.[45] Similarly, many law firms, for example, are looking at using community clouds to solve technology issues and share costs while still complying with confidentiality rules.[46] Like the private cloud, the community cloud offers heightened control over access to data, but again may come at a higher cost than a public or hybrid cloud.[47]

The third deployment type is the public cloud. The general public has access to the public cloud for a variety of uses, and it may be owned or managed by any combination of businesses, academic institutions, and government institutions.[48] The physical infrastructure of a pubic cloud is located on the cloud provider's premises.[49] Most concerns raised about the public cloud are held by policy-leaders and industry leaders[50] as they try to regulate the public's use of the cloud. In particular, this model comes at more of a heightened security risk than private or community clouds.[51] The benefit to public clouds is that they may have more state-of-the-art technology since large organizations operating the public cloud have more resources to invest.[52]

The final deployment model is the hybrid cloud, which can exist in any combination of two or three of the models (private, community, or public) but "remain unique entities. . .bound together by standardized or proprietary technology that enables data and application portability."[53]

Among the three service models and four deployment models of the cloud, there are many combinations that can be specifically tailored to meet the needs of each user, or groups of users, in order to provide the best

---

43. *Cloud Deployment Models, supra* note 39.

44. *Id.*

45. *Id.*

46. *See* LEGAL CLOUD COMPUTING ASSOCIATION, http://www.legalcloudcomputing association.org/ (last visited Jan. 2, 2013). Indeed, the market for law-related clouds have only begun to grow. The Legal Cloud Computing Association is a consortium of "leading cloud computing providers" who work together to establish practices and expectations in the legal cloud, collaborating with bar associations and other rule-making bodies to adapt clouds to specific legal-field needs. *Id.*

47. *Id.*

48. NIST, *supra* note 7.

49. *Id.*

50. Timothy D. 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 (2010).

51. *Cloud Deployment Models, supra* note 39.

52. *Id.*

53. NIST, *supra* note 7.

security while reducing the cost of infrastructure and enjoying the other benefits cloud computing has to offer.

C. Personal Jurisdiction and Fourth Amendment Concerns

Now that is it understood where and how data in the cloud may be stored and accessed by consumers and providers alike, an important question comes to mind: who owns data in the cloud? Because different networks of clouds may span across many states or even across nations, conflicting laws may govern the data and those who interact with it.[54] This Note does not attempt to wade through the complexities of all relevant ownership laws that may govern data in the cloud; instead, it examines and highlights the current issues in data jurisdiction laws to provide context regarding overall cloud computing regulations.

In at least one jurisdiction, an interaction through the cloud created sufficient "minimum contact" with a state to give a court personal jurisdiction over a defendant who otherwise may not have had sufficient minimum contact.[55] In *Forward Foods LLC v. Next Proteins, Inc.*, a New York trial court addressed the role of cloud computing in determining personal jurisdiction:

> In its personal jurisdiction analysis, the court made note of the fact that there was a virtual data room where Defendants uploaded documents for Emigrant to review in New York[.] This proved to be a significant factor in finding that defendants had maintained sufficient contacts with New York to be subject to personal jurisdiction.[56]

The New York court is not alone in recognizing a paradigm shift in how to treat data and property stored in the cloud.[57] In *State v. Bellar*, Judge Sercombe's dissent noted the drastic shift in privacy expectations and how the courts should respond:

> [A] person's privacy rights in electronically stored personal information [are not] lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving away from the storage of

54. *Privacy in the Cloud Computing Era: A Microsoft Perspective*, MICROSOFT (Nov. 2009), http://www.microsoft.com/download/en/details.aspx?id=24413.

55. Forward Foods LLC v. Next Proteins, Inc., 2008 NY Slip Op 52058U, 1 (N.Y. Sup. Ct. 2008).

56. Fernando M. Pinguelo & Bradford W. Muller, *Avoid the Rainy Day: Survey of U.S. Cloud Computing Caselaw*, 2011 B.C. INTELL. PROP. & TECH. F. 11101, 3 (2011).

57. *See generally* State v. Bellar, 231 Or.App. 80 (Or. Ct. App. 2009).

> personal data on computer hard drives to retention of that information in the "cloud" of servers owned by internet service providers. That information can then be generated and accessed by hand-carried personal computing devices. I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.[58]

The controlling law on cloud computing is patchwork at best, but the laws regulating the cloud and data jurisdiction are not the only aspect that are out-of-step with the digital age.[59] The Supreme Court has recently referenced the need for heightened protection for users in the digital age across the spectrum, especially with regard to Fourth Amendment concerns.[60] In *United States v. Jones*, police attached a GPS tracking device to defendant Jones' car without a warrant. The Court unanimously held that it was a search pursuant to the Fourth Amendment.[61] Notable, though, was Justice Sotomayor's concurrence, in which she rejected the notion that users have no reasonable expectation of privacy when they voluntarily give information:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 10, and perhaps not.[62]

These Fourth Amendment issues presented in data tracking and collecting

---

58. *Id.* at 110.

59. *Supreme Court Rules: Congress Needs to Bring Privacy Law into 21st Century*, DIGITAL DUE PROCESS (Jan. 29, 2012), http://www.digitaldueprocess.org/index.cfm?objectid=F6721970-4D0A-11E1-9791000C296BA163; United States v. Jones, 132 S.Ct. 945 (2012).

60. United States v. Jones, 132 S.Ct. 945 (2012) (Sotomayor, J., concurring).

61. *Id.* at 1, 3, 12.

62. *Id.* at 5. (Sotomayor, J., concurring).

cases are fascinating and complex, and certainly must be addressed by the legislature and courts in the future. Although the issue here is not discussed at length, an introduction helps to understand the scope of privacy and how it may intertwine with cloud computing in the future.

III. CURRENT UNITED STATES LAW

A. Electronic Communications Privacy Act of 1986

The law that currently governs cloud usage and data storage is the Electronic Communications Privacy Act of 1986 (ECPA).[63] The ECPA is broken down into three parts: Title I protects wire, oral, and electronic communications while in transit and amends the Wiretap Act; Title II covers the Stored Communications Act (SCA) which protects communications held in electronic storage (discussed in further detail below); and Title III restricts the use of devices that record dialed telephone numbers.[64] The ECPA was amended in 1996 to heighten privacy protection and place a higher standard on law enforcement.[65] The ECPA was also amended by the Communications Assistance to Law Enforcement Act (CALEA), the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization act in 2006, and the FISM Amendments Act of 2008,[66] but none of these revisions applied to the Stored Communications Act. The main problem with the ECPA is that it relies on language rooted in an outdated understanding of the word "communication."[67] Courts are split as to when the ECPA applies and when it does not, creating a fragmented, patchwork application of privacy laws.[68] For instance, the First Circuit held that copying emails from storage was a prohibited interception, but a federal district court ruled that because the government's keystroke logger was not used while the computer was connected to the Internet, the information captured was not an electronic communication.[69]

In *United States v. Councilman*, defendant Councilman ran a website for out-of-print books and also offered email accounts to book dealer customers.[70] Councilman instructed his employees to copy incoming emails from Amazon.com before they were routed to the user's mailbox so Councilman's business could read the message and have a competitive

63. Martin, *supra* note 50, at 305-307.

64. *Electronic Communications Privacy Act of 1986*, U.S. DEPT. OF JUST., OFF. OF JUST. PROGRAMS, http://it.ojp.gov/default.aspx?area=privacy&page=1285 (last updated Apr. 7, 2010).

65. Martin, *supra* note 50, at 305.

66. *Electronic Communications Privacy Act of 1986*, *supra* note 64.

67. Martin, *supra* note 50, at 301 (internal citation omitted).

68. *Id.* at 304-308.

69. *Id.* at 305-306.

70. United States v. Councilman, 418 F.3d 67, 70-71 (1st Cir. 2005).

advantage.[71] "Councilman contend[ed] that the e-mail messages he obtained were not, when procmail copied them, "electronic communication[s]," and moreover the method by which they were copied was not "intercept[ion]" under the Act."[72] The court looked to the legislative history of the ECPA to determine whether or not messages in transit, such as these, would fall into the 'interception' portion of the statute.[73] Ultimately, the court concluded "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act."[74]

The Ninth Circuit has also recently applied the ECPA, holding that the statute applied to non-citizens of the United States as well when their data was stored in the United States.[75] In *Suzlon Energy Ltd. v. Microsoft Corp.*, Microsoft was sued to produce emails for use against an Indian citizen in a civil lawsuit pending in Australia.[76] The Ninth Circuit held that the statute, on its face, precluded Microsoft's disclosure of the emails because protection of the ECPA strictly precluded disclosures for civil suits.[77] However, the court explicitly left open the question of what would happen if the data were stored on servers outside the United States.[78]

When drafting the ECPA, Congressional intent was to afford greater privacy protection to stored e-mails than subscriber information, and to regulate more heavily those services available to the public than services that have a more restricted audience.[79] The general intent was to afford greater privacy protection for greater privacy interests.[80] Today, though, Congress faces heavy criticism for failing to update the ECPA.[81] As the

---

71. *Id.* at 70-71.

72. *Id.* at 72.

73. *Id.* at 76.

74. *Id.* at 78.

75. Suzion Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011); *see also* Venkat Balasubramani, *9th Cir.: ECPA Protects Non-Citizen Communications Stored in the US – Suzlon Energy v. Microsoft*, TECH. & MARKETING L. BLOG (Oct. 4, 2011), http://blog.ericgoldman.org/archives/2011/10/9th_cir_ecpa_pr.htm.

76. *Suzion*, 671 F.3d at 731.

77. *Id.* at 730.

78. *Id.* at 729.

79. *Electronic Communications Privacy Act of 1986, supra* note 64.

80. *Id.*

81. Mark Gibbs, *While We Wait for Cold Fusion, Let's Update the ECPA*, NETWORK WORLD (Oct. 24, 2011 12:05 AM), http://www.networkworld.com/columnists/2011/102411-backspin.html?page=1; Alex Howard, *Senate Considers update to Electronic Communications Privacy Act*, GOVFRESH (Sept. 22, 2010 7:07 PM), http://gov20.govfresh.com/senate-considers-update-to-electronic-communications-privacy-act/; *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (testimony of Brad Smith, General Counsel, Microsoft Corp.), *available at* http://www.judiciary.senate.gov/hearings/

American Civil Liberties Union points out, at the time the ECPA was adopted, "there was no World Wide Web, nobody carried a cell phone, and the only 'social networking' two-year-old Mark Zuckerberg was doing was at pre-school or on play dates."[82] It is ironic that the law regulating Facebook is nearly older than Facebook's creator.

Another concern with the ECPA relates to the argument the Justice Department is making for the law to remain static and its interpretation of the current law:

> Last year. . . the Justice Department argued in court that cellphone users had given up the expectation of privacy about their location by voluntarily giving that information to carriers. In April, it argued in a federal court in Colorado that it ought to have access to some e-mails without a search warrant. And federal law enforcement officials, citing technology advances, plan to ask for new regulations that would smooth their ability to perform legal wiretaps of various Internet communications.[83]

Justice Sotomayor's concurrence in *Jones* rejects many of these arguments,[84] but until the entire court addresses these issues or the law is changed, some lower courts still may be persuaded by these arguments.

Several proposals to update the ECPA have been made, but there have been no significant revisions to the statute since its enactment.[85] Recently, the Senate Committee on the Judiciary heard testimony from many witnesses proposing change in the law.[86] Senator Patrick Leahy, who

---

testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary) *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Jan. 2, 2013).

82. *Modernizing the Electronic Communications Privacy Act*, ACLU, http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited Jan. 2, 2013).

83. Miguel Helft & Claire Cain Miller, *1986 Privacy Law is Outrun by the Web*, N.Y. TIMES(Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html?hp.

84. *See generally* United States v. Jones, 132 S.Ct. 945 (2012).

85. *About the Issue*, *supra* note 81; Sen. Patrick Leahy, *Leahy Introduces Benchmark Bill to Update Key Digital Privacy Law (Press Release)*, SENATE.GOV (May 17, 2011), http://www.leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29e3c5f758f2.

86. *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (testimony of the Hon. Cameron F. Kerry, General Counsel, U.S. Dept. of Commerce), *available at*

drafted the original ECPA, sponsored the legislation entitled the Electronic Communications Privacy Act Amendments Act of 2011.[87] The updated legislation would improve privacy protections for electronic communications and clarify legal standards by which the government could obtain this data. [88] Additionally, the proposal included enhanced privacy protections for emails and electronic communications which are searchable subject to warrants for probable cause.[89] Furthermore, in line with the *Jones* decision, the legislation included proposals for how to treat user location information collected through electronic devices.[90] Senator Leahy testified before the Senate Committee on the Judiciary saying:

> Since the Electronic Communications Privacy Act was first enacted in 1986, ECPA has been one of our nation's premiere privacy laws. But, today, this law is significantly outdated and out-paced by rapid changes in technology and the changing mission of our law enforcement agencies after September 11. Updating this law to reflect the realities of our time is essential to ensuring that our federal privacy laws keep pace with new technologies and the new threats to our security.[91]

While Congress has started to take notice of the need for change, perhaps the largest and most diverse group pushing for change of the ECPA

---

http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (testimony of the Hon. James A. Baker, Associate Deputy Att'y Gen.), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *Testimony of Brad Smith*, *supra* note 81; *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (testimony of Jamil N. Jaffer), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (testimony of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16302cc&wit_id=e655f9e2809e5476862f735da16302cc-0-0; *Testimony of the Honorable Patrick Leahy*, *supra* note 85.

87. *Bill Summary and Status, 112th Congress (2011-2012)*, LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.1011: (last visited Jan. 2, 2013); Berin Szoka & Charlie Kennedy, *Supremes to Congress: Bring Privacy Law into 21st Century*, CNET (Jan. 29, 2012 8:01 PM), news.cnet.com/8301-13578_3-57368025-38/supremes-to-congress-bring-privacy-law-into-21st-century/?tag=cnetRiver; Sen. Leahy, *supra* note 85.

88. Sen. Leahy, *supra* note 85.

89. *Id.*

90. *Id.*

91. *Id.*

is Digital Due Process Coalition, "a diverse coalition of privacy advocates, major companies and think tanks, working together."[92] Notable members of the coalition include: Adobe, Amazon.com, the American Civil Liberties Union, Apple, the Distributed Computer Industry Association, Dropbox, the Electronic Frontier Foundation, Facebook, Hewlett-Packard, Google, Intel, the Liberty Coalition, LinkedIn, Microsoft, Salesforce.com, and TRUSTe.[93] Several individuals from around the country, including many from the legal field, are involved as well.[94] In their push for change, the coalition has a goal

> [t]o simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.[95]

The relevant changes that need to be made to the ECPA noted above are generally revisions applicable to Title II regarding the Stored Communications Act.

B. The Stored Communications Act

Title II of the ECPA, known as the Stored Communications Act (SCA) has been applied most regularly to issues regarding cloud computing. The SCA "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses."[96] Interpretation of the SCA is difficult and confusing because its application to cloud computing hinges on the definitions of "electronic communication service" (ECS) and "remote computing service" (RCS), despite the definitions' outdated meaning in current contexts.[97] The SCA prohibits providers of ECS and RCS from disclosing electronic communications

92. *Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Jan. 2, 2013).

93. *Id.*

94. *Id.*

95. *Our Principles*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Jan. 2, 2013).

96. 18 U.S.C.A. §§ 2701-12 (West 2012); *see also Electronic Communications Privacy Act of 1986*, *supra* note 64.

97. Martin, *supra* note 50, at 306-307.

without consent, even to the government.[98]

Congress, in drafting the statute, sought to regulate two different types of computing functions: "1) electronic communication services (ECS) designed to handle 'data transmissions and electronic mail' and (2) remote computing services (RCS) intended to provide outsourced computer processing and data storage."[99] Data stored by RCS providers receives fewer privacy protections than communications held by ECS providers, but both ECS and RCS providers may voluntarily provide "personal identifying information about the user, such as her name, physical or e-mail addresses, and IP address. . .to any non-governmental entity or provide it directly to the government upon receipt of an administrative subpoena."[100] A user's information is generally protected from disclosure to private litigants in civil cases.[101] However, as seen in *Suzlon Energy Ltd.,* the question still is not fully resolved in the courts as to whether this privilege is absolute.[102]

By definition, the SCA requires that electronic communication services provide "the ability to send or receive wire or electronic communications."[103] Unfortunately, many cloud computing services today lack send and receive capabilities,[104] putting them outside the purview of this section's protections. The definition of "electronic storage" also is inapplicable to cloud storage.[105] The statute defines electronic storage as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[106] Due to these narrow definitions, the provisions of the SCA that protect ECS are inapplicable to cloud storage.[107]

Courts nonetheless have attempted to stretch the definitions provided in the ECPA. In *Quon v. Arch Wireless Operating Company*, the Ninth Circuit held that a pager-service was entitled to ECS protections despite the

98. *Id.* at 306.

99. Robison, *supra* note 13, at 1231-1232; 18 U.S.C.A. § 2510 (West 2012) (Defines electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

100. Robison, *supra* note 13, at 1208.

101. *Id.* at 1208-1209.

102. Suzion Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

103. 18 U.S.C.A. § 2510 (West 2012).

104. Robison, *supra* note 13, at 1209.

105. 18 U.S.C.A. § 2510 (West 2012) ((17) "electronic storage" means-- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication).

106. 18 U.S.C.A. § 2510 (West 2012).

107. Robison, *supra* note 13, at 1210.

fact that it did not fit into the statutory definitions.[108]

> The Ninth Circuit's reasoning in that case was tortured by a resort to legislative history from the 1980s that relied on the operation of outdated and obsolete technology. The court tried to distinguish between storage and communication services, but under the cloud computing model, those types of services are utterly indistinguishable.[109]

Without the types of revisions that Senator Leahy and the Digital Due Process Coalition are suggesting, courts will be forced to stretch the outdated laws, as the Ninth Circuit did, in a way that could apply even remotely to today's technology. For these reasons, it is time for Congress to update the controlling laws.

C. Computer Fraud and Abuse Act

The same year the ECPA was enacted, Congress enacted the Computer Fraud and Abuse Act (CFAA).[110] The CFAA makes it a crime to (1) knowingly commit computer espionage (against the United States government); (2) intentionally hack a computer for the purpose to obtain bank records; (3) intentionally access a United States government department or agency computer without authorization; (4) knowingly access a protected computer with an intent to defraud by obtaining something of value; (5) knowingly transmit a computer virus or worm to another computer that causes damage; (6) knowingly traffic passwords with the intent to defraud; or (7) threaten to damage another computer via extortion.[111] An attempt to do any of the above is also a crime.[112] When someone "accesses a computer used in or affecting interstate commerce without authorization or when that person exceed[s] authorized access" the CFFA is triggered.[113] The law is applicable to cloud computing when someone's information is stolen from the cloud, but fails to apply to or solve many of the difficulties surrounding cloud computing generally.

IV. PROPOSED AND RECENTLY-ENACTED UNITED STATES LEGISLATION

The 111th Congress Second Session introduced more than fifty pieces

---

108. Quon v. Arch Wireless Operating Company, 529 F.3d 892 (9th Circ. 2008).
109. Martin, *supra* note 50, at 307.
110. 18 U.S.C.A. § 1030(a) (West 2012), 18 U.S.C.A. § 2510 (West 2012).
111. 18 U.S.C.A. § 1030(a) (West 2012).
112. *Id.*
113. Mark H. Wittow, Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 J. Internet L. 1, 9 (2010).

of legislation that were cyber-related.[114] In response, the White House issued a legislative proposal in 2011 that focused on improving cyber security, infrastructure, and the federal government's own networks and computers.[115] The proposal opened up a line of communication between the White House and Congress relating to cyber issues, and focused Congress on issues needing to be addressed.[116] It also emphasized the critical need to address cyber-security vulnerabilities regarding national security, public safety, and economic prosperity.[117]

A. Chief Information Officer's Guidelines and Suggestions

The United States government has shown, through the Chief Information Officer's Guidelines and suggestions that regulating a large, multi-faceted cloud is possible, and indeed, large corporations are more than willing to adapt to the stringent security regulations if it means access to a particular consumer base. As such, the federal government has embarked upon moving over to a community-based cloud storage solution, partnering with Google for support.[118] Google has earned the Federal Information Security Management Act[119] certification necessary to handle government customer data, and the customer data is stored within the United States only.[120] In February 2010, the federal government implemented the Federal Data Center Consolidation Initiative (FDCCI) to reduce the number of storage facilities across the nation in favor of cloud computing.[121] Within the next four years, the government plans to have eliminated, reduced, or consolidated at least 800 data storage facilities as it moves to the cloud.[122]

---

114. Press Release, The White House, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

115. *Id.*

116. *Id.* at 5.

117. *Id.*

118. *FISMA-Certified Cloud Applications for Government*, GOOGLE, http://www.google.com/apps/intl/en/government/trust.html (last visited Jan. 2, 2013).

119. The Federal Information Security Management Act (FISMA) is Title III of the E-Government Act (PL 107-347), enacted December 2002. "FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." FISMA Detailed Overview, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, http://csrc.nist.gov/groups/SMA/fisma/overview.html (last visited Jan. 2, 2013).

120. *FISMA-Certified Cloud Applications for Government*, *supra* note 119.

121. Vivek Kundra, *Federal Cloud Computing Strategy*, CIO.Gov 8 (Feb. 8, 2011), *www.cio.gov/documents/federal-cloud-computing-strategy.pdf.*

122. *Id.*

The government has, for itself, taken several steps to ensure that any and all data it puts in its community cloud will be transparent between cloud providers and cloud consumers.[123] In 2010, the Federal Risk and Authorization Management Program (FedRAMP) established requirements for cloud computing security, "including vulnerability scanning, and incident monitoring, logging and reporting."[124] The goal along the way is to ensure that the shift to the cloud is met with confidence, trust, and security.[125] The NIST will "generate, assess, and revise a cloud computing roadmap on a periodic basis," and continue to develop and refine standards as innovation and technology evolve.[126]

This Note argues that how the federal government envisions the shift to, and privacy for, the cloud is also how the government should regulate all cloud users in the United States. The government recognizes the risks and benefits of using the cloud system for data, especially sensitive data, and has installed internal protections for its own. Congress should insist on nothing less than the same rigid standards the government employs to ensure compliance and protection of a user's data. Google's adaptations and willingness to receive accreditation is evidence that, if demanded, the industry can and will comply with security regulations.

B. Personal Data Protection and Breach Accountability Act of 2011

In addition to the proposed ECPA amendments previously discussed, Senator Richard Blumenthal introduced a bill entitled the Personal Data Protection and Breach Accountability Act of 2011.[127] The regulation would apply to companies who provide data storage to ten thousand or more customers.[128] Qualifying companies must adhere to strict storage guidelines and ensure that sensitive data is stored and protected; stiff penalties and fines could be levied against companies that do not comply.[129] Though the bill was proposed before Sony's massive data breach in the summer of 2011 that put the data of seventy-seven million consumers at risk, the Senator used the breach as further proof of why the law is needed.[130] Under the regulation, customers would be able to sue companies, such as Sony, that do not take adequate measures to prevent data breaches.[131] Much of this bill

123. *Id.* at 26.
124. *Id.*
125. *Id.*
126. *Id.* at 29.
127. Nick Bilton, *Senator Introduces Online Privacy Bill,* N.Y. TIMES (Sept. 8, 2011 7:27 PM), http://bits.blogs.nytimes.com/2011/09/08/senator-introduces-new-online-privacy-bill/.
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.*

was incorporated into the Data Breach Notification Act of 2011.

C. *Data Breach Notification Act of 2011*

Senator Dianne Feinstein proposed the Data Breach Notification Act of 2011 "to require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information."[132] If a breach occurs, the government body or the business that engages in interstate commerce is required to notify any user that may have been affected as well as the owner of the information that may have been collected.[133] In addition, businesses engaging in activities that violate the Act would be subject to a civil suit by the United States Attorney General in federal court with civil penalties.[134] State attorneys general would also be authorized to bring actions in state court to enforce the Act.[135] The bill died after being referred to the Senate Committee on the Judiciary in September 2011, necessitating a new proposal next session to advance the bill.[136]

D. *Microsoft's Cloud Computing Advancement Act*

In 2010, Microsoft's senior vice president and general counsel Brad Smith announced a proposal to both Congress and the information technology industry to adopt new standards for cloud computing.[137] The proposal was based on a survey conducted by Microsoft which found that fifty-eight percent of the general public and eighty-six percent of business leaders were excited about cloud computing, but ninety percent of those surveyed had concerns about security, access, and privacy of data in the cloud.[138] A majority of those surveyed also felt the government should enact rules regulating cloud computing.[139] The proposal called for improving privacy and data access rules, starting with the ECPA; modernizing the CFAA to allow law enforcement to deter and prosecute online-based crimes; establishing clear regulations that inform businesses and consumers on how information is collected and used online; and

---

132. S. 1408, 112th Cong. (2011), *available at* http://www.opencongress.org/bill/112-s1408/show.

133. *Id.*

134. *Id.* at Section 8.

135. *Id.*

136. *S. 1408: Data Breach Notification Act of 2011*, *supra* note 132.

137. *Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud,* Microsoft (Jan. 20, 2010), http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx [hereinafter Microsoft Urges].

138. *Id.*

139. *Id.*

building a new framework to encompass data access issues globally.[140] Microsoft's proposal also stresses the need for an updated ECPA to unify the ECS and RCS definitions since there is no longer a technological difference; and the proposal advocates for the elimination of unequal treatment of e-mails based on how long they have been stored.[141] Although nothing significant has happened with this proposal Brad Smith, Microsoft's general counsel, has been an advocate before the Senate petitioning for change.[142]

E. IBM and the Open Cloud Manifesto

International Business Machines Corporation (IBM) issued its own proposal on how to regulate the cloud in Spring 2009,[143] which Amazon.com and Microsoft flat-out rejected.[144] IBM's Open Cloud Manifesto is based on the premise that "[t]he industry needs an objective, straightforward conversation about how this new computing paradigm will impact organizations, how it can be used with existing technologies, and the potential pitfalls of proprietary technologies that can lead to lock-in and limited choice."[145] Supporters applauded IBM's step toward openness and early action to implement standards for the industry.[146] Microsoft, on the other hand, said "there were some things it agreed with in the [M]anifesto, but others that were either too vague or did not reflect its interests."[147] Ultimately, the Manifesto was drafted to begin the conversation about cloud computing, not to define cloud computing. The Manifesto now serves as a discussion point for corporations and industry experts.[148] As Microsoft has shown, though, the industry is unlikely to regulate itself unless it is in each of the companies' best interest;[149] government action would therefore be needed to regulate cloud providers for the sake of public interest.

---

140. *Id.*

141. *Id.*

142. *Testimony of Brad Smith*, *supra* note 81.

143. *Introduction*, OPEN CLOUD MANIFESTO, http://www.opencloudmanifesto.org/opencloudmanifesto1.htm (last visited Jan. 2, 2013).

144. Ina Fried, *Amazon, Microsoft Reject 'Open Cloud Manifesto,'* CNET (Mar. 27, 2009), http://news.cnet.com/8301-13860_3-10206077-56.html; Steve Hamm, *Meet the Open Cloud Manifesto*, BLOOMBERG BUSINESSWEEK (Mar. 30, 2009 12:01 AM), http://www.businessweek.com/technology/content/mar2009/tc20090329_463505_page_2.htm.

145. *Introduction*, *supra* note 143.

146. Fried *supra* note 144.

147. *Id.*

148. *Id.*

149. *Id.*

F. Cloud Computing Research Enhancement

Effective January 4, 2011, Congress enacted legislation directing the Nation Science Foundation (NSF) to research areas that affect public and private cloud computing, such as:

> (1) new approaches, techniques, technologies, and tools for-- (A) optimizing the effectiveness and efficiency of cloud computing environments, and (B) mitigating security, identity, privacy, reliability, and manageability risks in cloud-based environments, including as they differ from traditional data centers; (2) new algorithms and technologies to define, assess, and establish large-scale, trustworthy, cloud-based infrastructures; (3) models and advanced technologies to measure, assess, report, and understand the performance, reliability, energy consumption, and other characteristics of complex cloud environments; and (4) advanced security technologies to protect sensitive or proprietary information in global-scale cloud environments.[150]

This legislation will allow for the growth of both public and private clouds with government oversight. The NSF Director, in conjunction with the NIST, will also review companies' management of data to see that they comply with federal laws and regulations of cloud environments and the issues of piracy and misappropriation of cloud services.[151] These measures are steps in the right direction, but researching the issue in depth before acting perhaps will prove ineffective, as the technology may again change, advance, and take on new characteristics that may need to be addressed because they fall outside the purview of the NST's studies.

V. CURRENT EUROPEAN UNION LAWS REGARDING CLOUD COMPUTING

A. Global Industry Compliance with Local Laws, Generally

This Note argues that if nothing less is expected of cloud providers than stringent security and protection of users' privacy and data, then that is what a nation will receive. How other nations have demanded the industry adapt to the nation's laws, so should the United States. Amazon.com adapted their cloud services for the European Union by bringing storage systems to Ireland specifically in compliance with the European Union's

150. 42 U.S.C.A. § 1862p-12 (West 2012).
151. *Id.*

strict privacy laws.[152] Because the European Union requires physical data centers to be located within the borders of one of its member nations (with a few exceptions) companies must adapt to access the market.[153] Hewlett-Packard (HP) has followed Amazon.com's lead in adapting to the European Union's laws.[154] HP recognized that the benefits and impact of the cloud are so great that it was worth working within the existing framework and privacy laws in order to enter the market.[155] Outside the European Union and United States, companies are also complying with local laws. In Canada, for instance, IBM built a $42 million Compute Cloud Centre for Canadian businesses to develop, host, and test applications securely.[156] "Confidential information is protected and kept securely resident in Canada in accordance with Canadian privacy laws."[157] If the United States would act quickly, it too would reap the benefits of building a cloud infrastructure from the ground up, and have a say in how companies adapt to its laws.

B. Privacy Acts and Directives

In general, the European Union takes a more firm and protective stance for users' privacy than the United States. The European Union Data Privacy Directive controls the protection of personal data. The goal of Directive 95/46/EC is to strike a balance between high protection of individual privacy and free movement of data among those within the European Union.[158] "To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data."[159]

The Directive, enacted in 1995, creates rights for those individuals who have had personal information collected about them.[160] The individual must be notified with an explanation about who is collecting her information, who will have access to it, and why it is being collected.[161] If the data is used in marketing, the individual must have the opportunity to

152. *Amazon EC2 Crosses the Atlantic,* AMAZON.COM (Dec. 9, 2008), http://aws.typepad.com/aws/2008/12/amazon-ec2-crosses-the-atlantic.html.

153. Kevin J. O'Brien, *Cloud Computing Hits Snag in Europe*, N.Y. TIMES (Sept. 19, 2010), http://www.nytimes.com/2010/09/20/technology/20cloud.html?pagewanted=all.

154. *Id.*

155. *Id.*

156. *IBM Launches $42 Million Cloud Computing Centre in Canada, IBM (Jan. 31, 2011),* http://www.ibm.com/news/ca/en/2011/01/31/w431220f88404v59.html.

157. *Id.*

158. *Protection of Personal Data*, EUROPA, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm (last updated Jan. 2, 2011).

159. *Id.*

160. *Id.*

161. *Id.*

correct the information and object to the usage.[162] Stricter rules also govern sensitive information relating to racial and ethnic background, political affiliation, religious or philosophical beliefs, trade-union membership, sexual preferences, and health.[163] Before this information may be collected, the individual must give explicit consent.[164] There are exceptions to this rule for employment contracts, non-profit organizations, and the legal system, among other things.[165] The Data Privacy Directive created a basic legal framework, "including the default requirement of 'opt-in' consent to data sharing and the 'adequacy requirement' for data-sharing with non-EU companies. In response to this latter requirement, the U. S. negotiated a 'safe harbor' framework for U. S. companies doing business in Europe or with European companies."[166]

Critics of this directive are quick to describe it as a "top-down, bureaucratic model [that] imposes heavy costs and inconveniences on European businesses compared to the American system in which information flows freely and only harmful uses of information are prevented or punished. The Directive is also inconsistent in many respects with free speech."[167] Others also identified several weaknesses of the Directive, such as: links between personal data and real privacy risks are unclear; the methods used to provide data processing transparency are inconsistent and ineffective; data export and transfer rules controlling countries outside the European Union are outdated; accountability and enforcement of the Directive is inconsistent; definitions throughout the directive are too simple and static.[168] Still, some do find strengths in the Directive: it harmonizes data protection principles; it is technology neutral; and it improves awareness of data protection concerns.[169]

In 2002, the Directive on Privacy and Electronic Communications increased the strength of European Union privacy laws by putting further restrictions on the use of cookies.[170] This directive was again updated in 2009 "to strengthen the existing legal requirements concerning the 'clear and comprehensive' information that must be given to users."[171] However,

---

162. *Id.*

163. *Id.*

164. *Id.*

165. *Id.*

166. *The European Legal Context: the EU Privacy Directives,* LEGAL INFORMATION INSTITUTE, http://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives (last visited Jan. 2, 2013).

167. *The EU Data Privacy Directive,* PRIVACILLA.ORG, http://www.privacilla.org/business/eudirective.html (last visited Jan. 2, 2013).

168. NEIL ROBINSON ET AL., Review of the European Data Protection Directive (RAND CORP. 2009), *available at* http://www.rand.org/pubs/technical_reports/TR710.html.

169. *Id.*

170. Paul Lanois, *Privacy in the Age of the Cloud,* 15 J. Internet L. 3, 6 (2011).

171. *Id.* at 7.

neither update specifically addressed the issues surrounding cloud computing.

The European Commission ran a public consultation poll from May 16, 2011 through August 2011 about cloud computing in Europe.[172] Five hundred and thirty-eight responses were received, including 230 from companies, 182 from individuals, 42 from academics, 33 from public administrators, and 51 from respondents claiming "other."[173] Of these respondents, 86 individuals believed that an update to the EU Data Privacy Directive would be helpful to facilitate growth while protecting privacy, while 66 said it would not be helpful.[174] Responses from businesses were only marginally better, with 114 companies answering in the affirmative, and 89 answering in the negative.[175]

VI. PROPOSED EUROPEAN UNION LEGISLATION

A. European Cloud Computing Strategy

Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, has been very involved over the last few years in working to provide a comprehensive and actionable plan to grow and develop cloud computing in the European Union.[176] In setting an agenda to make Europe more cloud-friendly, the European Commission is developing a European Cloud Strategy (the Strategy), to be detailed specifically in mid-2012.[177] Part of the Strategy is to create a "European Cloud Partnership between public [entities] and private industries. . . to agree [on] common requirements for public Cloud procurement and thus harness the buying power of the public sector. So the Cloud can support

172. European Commission, Information Society and Media Directorate-General, *Cloud Computing: Public Consultation Report* (Dec. 5, 2011), *available at* http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7663.

173. *Id.*

174. *Id.*

175. *Id.*

176. *See generally*, Press Release, Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda EU Data protection reform and Cloud Computing "Fuelling the European Economy" event, *Microsoft Executive Briefing Centre Brussels* (Jan. 30, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en [hereinafter Kroes: *Fuelling the European Economy*]; Neelie Kroes, *Vice President of the European Commission*, EUROPA, http://ec.europa.eu/commission_2010-2014/kroes/ (last visited Oct. 4, 2012); *Cloud Computing: A Legal Maze for Europe*, EURACTIV (Feb. 11, 2011), http://www.euractiv.com/innovation/cloud-computing-legal-maze-europe-linksdossier-502073; Jack Clark, *Kroes Calls for Better EU Cloud Security*, ZD NET (Nov. 25, 2010 5:16 PM), http://www.zdnet.co.uk/news/cloud/2010/11/25/kroes-calls-for-better-eu-cloud-security-40090987/.

177. Kroes: *Fuelling the European Economy*, *supra* note 176.

public administrations and public administrations can support the Cloud."[178] The European Commission also has proposed a unified Regulation, as opposed to further Directives,[179] that would impose a single set of rules for Europe and a single enforcement agency across all 27 member states.[180] This would allow companies based in Germany hosting servers in England, Ireland, and France to have one moderating agency; it would also apply consistent rules to providers based outside of the European Union.[181] The focus would be on the data, not on the location of the server, recognizing the fact that it is a very interconnected world and clouds cross borders.[182]

In addition, "[t]he plan includes fines of as much of 2 percent of annual global sales for companies mishandling or losing personal data, as well as a requirement to report serious data breaches within 24 hours."[183] However, companies are balking at the 24-hour notice requirement because many companies do not find out about breaches within such a short amount of time.[184] Companies applaud the efforts to make the laws balanced, but they would like to have some input in designing the regulations as well.[185]

The European Cloud Partnership (the Partnership) that Vice President Krose proposed will have €10 million ($13 million) of initial funding.[186] Set out in three phases, the Partnership will first develop common requirements for cloud procurement, focusing on standards, security, and competition; next, it will provide solutions for the requirements imposed; and then it will build the actual structure of the new cloud.[187] Interestingly, this model is

178. *Id.*

179. Directives specify certain end-results that must be achieved by every member state and each member state is free to decide how this will be done. *Application of EU Law – What are EU Directives?,* EUROPEAN COMMISSION, http://ec.europa.eu/eu_law/introduction/what_directive_en.htm (last visited Jan. 2, 2013). EU regulations are binding upon each member state; nothing must be done to have them further implemented and applied. *Application of EU Law – What are EU Regulations?,* EUROPEAN COMMISSION, http://ec.europa.eu/eu_law/introduction/what_regulation_en.htm (last visited Jan. 2, 2013).

180. Kroes: *Fuelling the European Economy, supra* note 176.

181. *Id.*

182. *Id.*

183. Cornelius Rahn, *EU Seeks Joint National Cloud-Computing Purchase for Growth,* BLOOMBERG BUSINESSWEEK (Jan. 27, 2012 1:43 PM), http://www.businessweek.com/news/2012-01-27/eu-seeks-joint-national-cloud-computing-purchases-for-growth.html.

184. *Id.*

185. *Id.*

186. Jennifer Baker, *Europe Stumps up £8 Million for Cloud Computing Strategy,* COMPUTERWORLD (Jan. 27, 2012 3:30 PM), http://www.computerworlduk.com/news/public-sector/3333257/europe-stumps-up-8-million-for-cloud-computing-strategy.

187. Press Release, Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland (Jan. 26, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=0&language=EN&guiLanguage=en [hereinafter Kroes: Davos, Switzerland].

based on the United States federal government's shift to the cloud.[188] To quell fears of the European Union creating a super-cloud, Vice President Kroes made the point very clear: the need for cloud suppliers and publicly-run data centers should be determined by the efficiency considerations in the market; cloud infrastructures would not be built outright or by forcing more integration of current cloud infrastructures without market demand.[189] The large-scale announcement of the Partnership and further regulations to be promulgated from the European Commission will be released in mid-2012, with the first visible results sometime in 2013.[190]

B. European Economic and Social Committee on Cloud Computing in Europe

Though Europe has been more proactive in updating regulations of the cloud, it still has a long way to go.[191] The European Economic and Social Committee (EESC) wrote an opinion on its own initiative about cloud computing in Europe.[192] The purpose of the opinion was twofold:

> Using the Europe 2020 strategy and in particular its Digital Agenda as a starting point, the Committee has set out to examine an IT solution that is still undergoing significant, rapid development, holding out great promise for the future: cloud computing . . . . This opinion firstly aims to gather and share the concrete experiences of stakeholders and the [cloud computing] market. Secondly, it seeks to put forward a list of recommendations as to how to encourage Europe to position itself at the forefront of this promising sector, helped by leading companies in the sector.[193]

In drafting the opinion, the EESC noted that there are many flaws and weaknesses of the current cloud atmosphere: there are a number of standards designed to regulate and control cloud computing; there is no unified, identifiable, governing authority to enforce regulations; there is a lack of information available to users to understand the risks and benefits of

---

188. *Id.*

189. *See id.*

190. *Id.*

191. *Cloud Computing: A Legal Maze for Europe*, *supra* note 176.

192. Opinion of the European Economic and Social Committee on 'Cloud computing in Europe' (own-initiative opinion) 24/40, 2012 O.J. (C 24/08), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0040:0047:EN:PDF [hereinafter *Own-Initiative Opinion*].

193. *Id.* (footnote omitted).

cloud computing at various levels; there exists an "intrinsically fragile nature of the Internet (interrupted service due to incidents, cyber attacks etc.);" there are outsourcing risks inherent to data processing by a third party and outsourcing risks to nations that have another system of law; and the rights and obligations both of users and providers are still unclear in many respects.[194]

Despite these identified weaknesses, the EESC also identified many strengths of the cloud in the European Union and provided a number of recommendations to grow the cloud.[195] In particular, the EESC recommended: encouraging or subsidizing larger server farms in the European Union; public partnerships to encourage research centers in Europe to coordinate their developments; including public and private players in developmental rules and regulations; and "capitalizing on the EU's competitive advantage in the field of data security and privacy protection to ensure their strict application in the area of [cloud computing]."[196]

C. European Network and Information Security Agency Recommendations

The European Network and Information Security Agency (ENISA) was created by the European Union to "advance the functioning of the internal market."[197] In 2009, ENISA completed a Cloud Computing Security Risk Assessment, which concluded, "the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences [sic] can be more robust, scalable and cost-effective."[198] In the report, ENISA also recommended steps that users could take when choosing a cloud provider, including:

> inquiring about (1) personnel security (background checks, etc.); (2) supply-chain management (subcontractor arrangements); (3) operational security (change control procedure, updates, and network architecture controls); (4) authorization and authentication; (5) asset management; (6) continuity management (disaster recovery, incident management, and escalation); (7) physical security; and (8)

194. *Id.*
195. *Id.*
196. *Id.*
197. *Cloud Computing Benefits, Risks, and Recommendations for Information Security,* ENSIA, 2 (Nov. 2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.
198. *Id.*, at 3.

> legal requirements (location of data, governing jurisdiction, data recovery upon termination, subcontracts, and the like).[199]

The ENISA report focused its legal recommendations on issues that will arise through contract evaluation or contract negotiations between different providers. It sees many issues in cloud computing being resolved through contracts, but standard contract clauses may be unworkable due to the nature of cloud computing.[200] The report stresses that contract negotiators pay particular attention to rights and obligations of each party when there is a security breach, or what access should be granted to law enforcement authorities. Additionally, standard limitations of liability need to be revisited to properly reflect the role of each party in the usage of the cloud.[201]

D. Slow Growth of the Cloud Due to Strict Privacy Laws

Because of all the proposed legislation and action that the European Union is contemplating regarding cloud computing, the emerging clouds throughout the 27 member European Union have developed slower than those in the United States.[202] The existing EU regulations are cumbersome enough that an AT&T spokesperson warned that the European Union should not attempt to "over-regulate" due to the constantly changing nature of the cloud computing market.[203] Indeed, the privacy laws are so stringent that a law to be proposed in January 2012 would make it difficult for SaaS social media sites such as Facebook to operate in compliance with European Union law without significant changes on the company's part.[204] With this in mind, the European Union must strike a balance to both effectively protect user's privacy while not restricting the free flow of data that epitomizes cloud computing. The right balance has yet to be struck.[205]

Bob Lindsay, HP's European privacy director, stressed that "[t]here are restrictions on cloud computing in Europe . . . slowing its evolution, compared with what is taking place in the United States."[206] Users in the European Union also face a restricted network of clouds because the

---

199. Martin, *supra* note 50, at 39.

200. *See Id.*

201. *Id.*

202. O'Brien, *supra* note 154.

203. Valentina Pop, *Cloud Providers Warn Against EU 'Over Regulation'*, EUOBSERVER (Nov. 10, 2011 6:11 PM), http://euobserver.com/1018/113871.

204. *See* Anna Leach, *Upcoming EU Data Law Will Make Europe Tricky for Facebook*, THE REGISTER (Nov. 8, 2011), http://www.theregister.co.uk/2011/11/08/eu_new_data_protection_proposals/.

205. *See generally*, O'Brien, *supra* note 154.

206. *Id.*

European Commission refuses to allow the physical location of servers to be outside member nations, except for a few exceptions.[207] The United States, Argentina, and Canada are all approved to provide cloud computing services to the European Union; other nations such as Israel and Andorra have applied for approval.[208] If a company does not apply for approval, or if it is denied, that nation must negotiate and enter into a binding service level agreement with data processors to ensure that the personal information of European Union citizens will be handled in accordance with European Union regulations.[209]

VII. RECOMMENDATIONS

The current problems facing cloud computing are: jurisdictional control of data; Fourth Amendment concerns; outdated laws that are inapplicable to modern technology; and the ever-pervasive problem that technology will always outpace the laws. This Note argues that the United States should follow the European Union's lead and act quickly to influence cloud providers from the start; that Congress should update the ECPA; that Congress should update the CFAA; that Congress should update other outdated and rigid laws that are applied clumsily by courts around the country with more fluid guidelines adaptable to changing technology; and that Congress should allow enforcement acts to be brought in federal court exclusively to allow a more uniform system of enforcement.

It is evident that the United States and the European Union have taken different approaches in trying to regulate cloud computing. Despite this, in September 2011, some of the information technology players from the United States and European Union participated in a joint conference, sponsored by the European Commission Information Society and Media, the Network of European CIOs, EuroCloud, and NIST to "[d]rill down the issues of standards for cloud computing from [three] major angles: [p]olicy[,] [i]ndustry and markets (supply and demand side)[;] [s]tandards and interoperability; [and] [g]ather elements to devise a standards roadmap for [the European Union], including priorities, players, and processes."[210]

With international interest to streamline the cloud, this would be an ideal time for the United States government to enact regulations regarding cloud computing, while it is still blossoming. Like the European Union has done, the United States government would be able to dictate to corporations how to build a safe, secure cloud for users.

---

207. *Id.*

208. *Id.*

209. *Id.*

210. ETSI, *Standards in the Cloud: A Transatlantic Mindshare*, http://www.etsi.org/WebSite/NewsandEvents/2011_09_STANDARDSINTHECLOUD.aspx (last visited Jan. 2, 2013).

One study polling 127 cloud service providers across the United States and European Union found some disturbing trends: the majority of cloud providers believe it is their customer's responsibility to secure the cloud, not their own; on average, less than ten percent of the provider's operational resources were dedicated to security; providers feel that users flock to the cloud because of the low cost and faster application deployment; users do not choose the cloud based on security; and the majority of providers do not have dedicated security personnel.[211] The most concerning finding, though, was that the majority of cloud providers did not believe security is one of their most important responsibilities and they do not believe their products or services protect consumer's information, but are pondering the option of charging an additional fee for "security" of information at a later point in time.[212]

By updating the ECPA, the United States could prevent users from having to pay a service charge for security from cloud storage providers by making it an inherent part of the service. By amending the controlling laws, Congress could assure users that providers would make security a priority, not an add-on that could be charged as an extra fee and be simply an additional source of revenue for the provider. Additionally, modernization of the ECPA could protect against seizures of hardware from cloud providers that contain data from multiple users, except in rare circumstances. It is almost unthinkable to Jane Doe in Indiana that, because Joe Smith in California stored information in Amazon.com's cloud storage, the government's legal collection of Smith's data would include collection of any of Doe's unrelated information stored on the same server.

Congress should also update the CFAA to ensure consumers are protected in case of a security breach and provide explicit civil penalties for companies who fail to protect user privacy. The justification is two-fold: the money collected would provide remedial damages payable to those users who have been affected, and the damages would also act as a deterrent to companies who might otherwise keep their security systems lax.

If the United States were to act now while the metaphorical iron is hot, instead of waiting years for various departmental investigational reports to come back, the advantages would be huge. It is easier to shape an emerging technology from inception than try to change it later on. If it is understood from the beginning that providers must comply with data privacy laws, perhaps we will not have to face the possibility of an unsecure cloud.

Additionally, if the United States steps up now to encourage

211. Ponemon Institute, *Security of Cloud Computing Providers Study* 1, (2011), *available at* http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf.

212. *Id.*

protection of users' privacy, privacy acts could become uniform throughout jurisdictions across the world. Patchwork security is unacceptable, unstable, and confusing. Arguments that it is simply too expensive or impractical to ensure security in public clouds fail, because such security measures have been implemented successfully in moving the United States federal government to a community cloud backed by Google. Uniform privacy laws would allow servers to be located throughout the world, in nations that agree to uniform standards and help regulate the jurisdictional and ownership issues that arise. It would ease strain on courts, reduce international disagreements, and foster better security for users, regardless of where they, or their data, are located.

This Note proposes that Congress should allow enforcement actions in violation of the ECPA, CFAA, and any other legislation dealing with cloud computing to be brought exclusively in federal court to allow a more uniform system of interpretation and enforcement. Additionally, due to the redundant nature of data storage, the same information uploaded in New York could be copied on host servers not only within the same state, but also in North Carolina, California, and Illinois, all unbeknownst to the user. Exclusive jurisdiction in federal courts would be consistent with enforcement of patents, trademarks, and copyright – other highly fluid, nuanced, and technical fields. Exclusive jurisdiction in federal courts would also reduce the ability of companies to bury forum clauses in End User License Agreements or Terms of Service that work strictly to the company's advantage. Congress should reject concurrent jurisdiction in favor of uniform interpretation of the federal statutes and for sensitivities to federal policies in an area that is likely to have impact on users and companies on a global level.

Finally, the largest advantage that the United States would gain in adapting new laws of the cloud is replacing the old, outdated, fragmented laws that currently govern. Although courts strive to adapt laws to modern situations, most laws simply were not written to address many issues that arise today. Technology has, and always will, progress faster than laws. Common technologies now were not even considered twenty years ago when the laws were written. By adopting a modern, updated, forward-thinking approach, users may feel secure while stability may flow from courts in applying laws that are written to fit the technology. Justices and judges no longer will have to write concurrences hinting to Congress to update outdated laws. Several interest groups comprised of industry leaders, legal scholars, and real-world users have all expressed interest and enthusiasm in helping to update the laws, and they will prove to be valuable resources to Congress in updating the ECPA, CFAA, and drafting any other legislation that will be necessary to regulate the cloud, if Congress is willing to accept the help.

VIII. CONCLUSION

Cloud computing is an evolving technology that has outgrown and outpaced modern laws across the world regarding data storage, jurisdiction, and ownership. The United States' controlling law over clouds, and data in the cloud, was enacted more than two decades ago and has created a fragmented, patchwork law across the nation as courts try to apply outdated laws with modern technology. While efforts have been made to update the ECPA and other related laws, none yet have been passed or enacted. There is large support from legal scholars, industry leaders, and technology interest groups to update the legislation to provide a clearer framework not only for providers, but for users of the cloud as well. The United States government has implemented a strategy to shift much of itself to its own community cloud in partnership with Google, showing that it is possible to have a large, secure cloud that is available to users nationwide. Proposed strategies on how to handle the transition to the cloud are in the works, but none are nearly close enough, nor workable yet, to implement into law.

The European Union, on the other hand, already has a large framework requiring companies' strict adherence in protecting user privacy. Based on this, the European Union has been able to develop policies yet to be implemented, that have privacy at the forefront. The European Union is working on implementing regulations across all twenty-seven member states that would provide one centralized, unified regulatory body that regulates providers and users under one standardized regulation for operation. Both the United States' and European Union's proposals have merit, but action should be taken now, in the budding stages of growth, to establish a framework of regulations to support the cloud, instead of trying to add them in later.