A CLOUDY FORECAST: DIVERGENCE IN THE CLOUD COMPUTING LAWS OF THE UNITED STATES, EUROPEAN UNION, AND CHINA

Tina Cheng[*]

TABLE OF CONTENTS

[*] J.D., University of Georgia, 2013; B.A. University of California, Los Angeles, 2008.

I. INTRODUCTION

In early 2011, China announced plans to build a "city-sized cloud computing and office complex that will include a mega data center," signaling a rapid growth in information technology (IT) spending.[1] Meanwhile, Facebook is building a 300,000-square-foot "server farm" in northern Sweden to store the personal data of its European users.[2] In late 2011, U.S.-based company Amazon.com announced the release of its Kindle Fire tablet, a device that not only backs up all of the user's information in the cloud, but also uses the cloud to log all of that user's activity.[3]

As the world becomes increasingly digitalized, concerns arise about the security and privacy of personal and commercial information. This information is being steadily moved to "the cloud," an Internet-based service that "provide[s] consumers with vast amounts of cheap, redundant storage and allow[s] them to instantly access their data from a web-connected computer anywhere in the world."[4] However, this convenience comes with risks such as exposure to hackers and privacy invasion.

This Note will argue that the government regulations currently in place in the U.S., European Union (EU), and China are inadequate to protect the privacy of cloud consumers. The Note begins by defining cloud computing and its ramifications on the privacy of its users. It will then set out laws that govern cloud computing in the U.S., EU, and China, and demonstrate how they are outdated and insufficient to protect cloud users. Finally, this Note will recommend that countries adopt a uniform, updated definition of cloud computing while continuing to develop privacy policy according to their own national and regional interests.

---

[1] Patrick Thibodeau, *China Building a City for Cloud Computing*, COMPUTERWORLD.COM (Feb. 7, 2011, 5:59 AM), http://www.computerworld.com/s/article/9208398/China_building_a_city_for_cloud_computing.

[2] Rob Waugh, *That's Really Cool: Facebook Puts Your Photos into the Deep Freeze as It Unveils Massive New Five Acre Data Center Near Arctic Circle*, DAILY MAIL (Oct. 28, 2011, 9:48 AM), http://www.dailymail.co.uk/sciencetech/article-2054168/Facebook-unveils-massive-data-center-Lulea-Sweden.html#ixzz1dYknZf9L.

[3] David Behrens, *Tech Talk: New Kindle under a cloud*, YORKSHIRE POST (Oct. 24, 2011), http://www.yorkshirepost.co.uk/lifestyle/indoors/gadgets-and-tech/tech_talk_new_kindle_under_a_cloud_1_3896956.

[4] Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 360–61 (2010).

II. CLOUD COMPUTING

A. Defining Cloud Computing

The cloud computing model is perceived to be "the future of computing."[5] However, a debate exists over the formal definition of "cloud computing."[6] The National Institute of Standards & Technology describes 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] Generally speaking, cloud computing is the idea that software and data can be accessed as a service on the Internet rather than stored locally on one's own computer.[8] Cloud computing pledges to overcome problems presented by the "dispersed computing" structure, the traditional model of computing in which each user stores and accesses his personal information on one computer.[9] Electronic mail was the first to transition,[10] closely followed by companies like Google, Amazon, and eBay.[11] The global cloud computing industry is still developing, with a majority of technology experts predicting that by 2020 "most people will access software applications online and share and access information through the use of remote server networks."[12]

B. Benefits of Cloud Computing

Cloud computing offers five major benefits to both commercial and individual consumers: reduced cost, increased storage, alleviated the depended on information technology (IT) personnel, augmented reliability,

---

[5] *Id.* at 364.

[6] William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 BUS. LAW. 237, 237 (2010).

[7] PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COMMERCE, THE NIST DEFINITION OF CLOUD COMPUTING, SPEC. PUBL'N 800-145, at 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

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

[9] William J. Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Store Communications Act*, 98 GEO. L.J. 1195, 1200 (2010).

[10] Soghoian, *supra* note 4, at 363.

[11] Denny, *supra* note 6, at 237.

[12] Janna Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET (June 11, 2010), http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts.

and expanded accessibility.[13] First, most cloud services are "either free or significantly cheaper than more traditional desktop offerings."[14] Second, cloud computing has eliminated user concerns about a computer's storage capacity, memory, and updates since applications run directly from the cloud.[15] Thus, hard disk space that would have been taken up by traditional software is available for other uses.[16] Third, business users benefit because IT personnel no longer need to be concerned with keeping software up to date.[17] Fourth, cloud-based services regularly back up files stored on multiple servers so that users never have to worry about losing their data in the event of a hardware failure.[18] Fifth, cloud-based systems allow users to access their information from anywhere in the world where there is an Internet connection.[19]

C. Privacy Issues in the Cloud

Although cloud computing offers many advantages to business and consumer users, significant risks come with the massive amounts of sensitive data handled by cloud providers.[20] One such risk is vulnerability to computer hackers as user data is often transmitted via unencrypted network connections, making the access to obtain users' private information easy for hackers.[21] Although encryption protecting against hackers is used in some cases of lower-priority cloud services such as email, it only applies during the initial login phase and not during subsequent data transfers.[22] For example, the risk of data breach is increased when users are connected to unsecured public wireless networks, such as those at coffee shops.[23] In addition, because a cloud provider might store the data of multiple users on the same physical equipment, cloud users face the risk of isolation failure,

---

[13] Soghoian, *supra* note 4, at 365; *see also Six Benefits of Cloud Computing*, SYS-CON MEDIA (Nov. 3, 2008, 6:30 AM), http://web2.sys-con.com/node/640237 (listing six ways in which the public sector and government IT organizations could benefit from cloud computing).

[14] Soghoian, *supra* note 4, at 366.

[15] Lanois, *supra* note 8, at 29–30.

[16] *Id.*

[17] *Six Benefits of Cloud Computing*, *supra* note 13.

[18] Soghoian, *supra* note 4, at 366.

[19] Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 622 (2011).

[20] Denny, *supra* note 6, at 238.

[21] Soghoian, *supra* note 4, at 372.

[22] *Id.*

[23] *Id.* at 373.

i.e., an attack on one person may lead to a "guest-hopping" attack as a result of the inadvertent or intentional commingling of data.[24]

A factor that exacerbates this issue is the changing societal attitude toward online privacy.[25] Younger users "have much less concern about online privacy than older generations," and "are more likely to embrace the Internet's interconnectedness and convenience by participating in social networking, sharing digital content, and using cloud services."[26] To them, "values such as cost, convenience, efficiency, and networking" outweigh privacy concerns.[27]

Cloud users also face possible exposure from cloud providers.[28] Institutions such as banks and online merchants are legally liable for online fraud, so they have an incentive to encrypt customers' data as it is transmitted over the Internet.[29] Cloud providers, however, have no such liability concerns even though an email account may have information that is just as sensitive as the information in a bank account.[30] One way cloud providers could be forced to standardize encryption is through market pressure. However, due to "widespread (yet understandable) ignorance" of most users[31] and the current societal attitudes,[32] "[t]here simply isn't sufficient market demand for these providers to allocate the considerable financial and engineering resources required to [provide] encryption by default for all of their products."[33]

Since data is stored on servers worldwide, cloud-based services also bring into play the question of jurisdiction.[34] The existing legal structure intended to protect data that flows around the globe is insufficient to protect end users.[35] Data privacy laws are not globally uniform, and, as such, "data that might be secure in one country may not be in another."[36] The determination

---

[24] Timothy D. Martin, *Hey! You! Get Off 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, 296–97 (2010).

[25] Robison, *supra* note 9, at 1237.

[26] *Id.*

[27] *Id.*

[28] Soghoian, *supra* note 4, at 378.

[29] *Id.*

[30] *Id.* at 379.

[31] *Id.* at 380.

[32] Robison, *supra* note 9, at 1237.

[33] Soghoian, *supra* note 4, at 380.

[34] Lanois, *supra* note 8, at 44; *see also* Kevin J. O'Brien, *Cloud Computing Hits Snag in Europe*, N.Y. TIMES, Sept. 19, 2010, at B4 (noting that India and Malaysia are "growing hubs for cloud computing data centers").

[35] O'Brien, *supra* note 34.

[36] David Binning, *Top five cloud computing security issues*, COMPUTERWEEKLY.COM (Apr. 24, 2009, 2:36 PM), http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-

of whose law applies to information stored in the cloud may depend on factors such as "the type of user, the location of the user's computer, the location of the cloud provider's server(s), or some combination of these variables."[37] Due to these variables, a user's privacy may "vary significantly with the terms of service and privacy established by the cloud provider," leading to the abuse and exploitation of that user's information.[38]

Another threat to consumer privacy stems from the "ease with which the government can force an application provider to insert a backdoor or flaw in its own products."[39] For example, China, notorious for its rigid censorship of the Internet,[40] recently demonstrated the extent to which the government could regulate Internet activities. Skype is a "voice-over-IP software program that lets users make free peer-to-peer phone calls and conduct instant messaging over the Internet."[41] In China, Skype operates through TOM-Skype, a joint venture with Tom Group, and it dominates the Chinese market.[42] The year after TOM-Skype was released, the company admitted that the software contained "a filtering mechanism that prevents users from sending text messages that include banned phrases such as 'Falungong' and 'Dalai Lama.' "[43] Skype executives then confirmed that they had simply been complying with local Chinese law, and that other cloud providers such as Microsoft and Yahoo had all done the same.[44] Although government intrusion was a risk before the era of cloud computing, "it has been made more effective, and more difficult to discover through the shift to cloud-delivered software."[45]

cloud-computing-security-issues.htm#4.

[37] Barry Reingold et al., *Cloud Computing: Whose Law Governs the Cloud? (Part III)*, CYBERSPACE LAW., Jan.–Feb. 2010, at 1, 1.

[38] Lanois, *supra* note 8, at 44.

[39] Soghoian, *supra* note 4, at 423.

[40] *See China Tightens Internet Controls*, BBC NEWS (Feb. 23, 2010, 12:32 PM), http://news.bbc.co.uk/2/hi/8530378.stm (noting that China practices "extensive censorship" of the "world's biggest online population).

[41] Soghoian, *supra* note 4, at 407–08.

[42] Sui-Lee Wee & Chris Buckley, *Skype's Partner Says It Is Legal in China*, REUTERS (Jan. 4, 2011, 9:37 AM), http://www.reuters.com/article/2011/01/04/us-china-skype-idUSTRE7031DR20110104.

[43] Soghoian, *supra* note 4, at 408.

[44] *Id.*

[45] *Id.* at 423–24.

III. DATA PRIVACY LAWS AND THE NEED FOR REFORM IN THE UNITED STATES, EUROPEAN UNION, AND CHINA

A. European Union

In approaching the privacy issues surrounding cloud computing, the EU has focused on privacy as a fundamental right[46] in developing "minimum standards for the E.U. member states' . . . data privacy legislation."[47] The 1995 European Union Data Protection Directive 95/46/EC (EU Directive)[48] "standardized the requirements for the protection of personal information across all the countries within the EU."[49] Specifically, the EU Directive:

> 1. limits organizations' right to collect personal information, including restricting the amount of information to be gathered and limiting such collection to a specific permitted purpose;
> 2. requires certain organizations to obtain the consent of the data subject prior to using the personal data or disclosing such data to a third party; and
> 3. regulates transborder flows of personal data, effectively prohibiting organizations from exporting personal data to countries without adequate privacy laws (which includes the United States).[50]

The EU Directive was superseded in 2002 by the Directive on Privacy and Electronic Communications (2002 ePrivacy Directive).[51] As continuation of earlier privacy legislation policy efforts, the 2002 ePrivacy Directive sets forth two main obligations: first, providers of electronic communications services "must take appropriate technical and organi[z]ational measures to safeguard security of its services,"[52] and, second, EU member states are required to maintain confidentiality of

---

[46] Lanois, *supra* note 8, at 37.

[47] Vadim Schick, *Data Privacy Concerns for U.S. Healthcare Enterprises' Overseas Ventures*, 4 J. HEALTH & LIFE SCI. L. 173, 180 (2011).

[48] Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC).

[49] Lanois, *supra* note 8, at 37.

[50] Schick, *supra* note 47, at 180.

[51] Council Directive 2002/58, Directive on Privacy and Electronic Communications, 2002 O.J. (L 201) 37 (EC).

[52] *Id.* art. 4(1).

personal information.[53] More importantly, member states must restrict "listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users"[54] unless the user is "provided with clear and comprehensive information."[55] Although the update of the EU Directive was a step forward in privacy legislation, it did not provide guidance about "how and when the opportunity to refuse the storage of, or access to the information, needs to be given, leaving each EU Member State . . . free to provide its own interpretation on these issues."[56]

In 2009, the 2002 ePrivacy Directive was amended to increase individual privacy protections.[57] One major change in the 2009 ePrivacy Directive is the amendment of Article 5(3), which now provides:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information . . . about the purposes of the processing.[58]

Experts are split regarding the actual application of this change and how it relates to the rest of the Directive. One view is that Article 5(3), requiring the user's consent, conflicts with the Preamble of the Directive, which refers to both the "right to refuse" and "consent."[59] The Preamble states that users "engaging in any activity which could result in such storage or gaining of access" must have a "right to refuse" the obligation to provide information after being presented with "clear and comprehensive information" regarding such information.[60] Another term requires "the user's consent to processing."[61] A right to refuse can be viewed as an "opt-out," in which "an activity occurs unless the user stops the processing and indicates his opposition."[62] In contrast, consent is an "opt-in," which "implies that no

---

[53] *Id.* art. 5(1).
[54] *Id.*
[55] *Id.* art. 5(3).
[56] Lanois, *supra* note 8, at 16.
[57] Council Directive 2009/136, 2009 O.J. (L 337) 11–36 (EC).
[58] *Id.* art. 2(5).
[59] *Id.* art. (66).
[60] *Id.*
[61] *Id.*
[62] Francoise Gilbert, *2002 EU Directive on Privacy and Electronic Communications (As*

activity can occur unless the user has done some act that expresses his consent."[63] The varying interpretations of the terms in the amended Article 5(3) and Preamble "may result in significant discrepancies in the laws of the different Member States, the opposite effect . . . of a directive."[64] Another view concerning the inclusion of both of these terms is that the EU meant to "emphasize that the user must be presented with a clear choice and must be able to give 'any freely given specific and informed indication of his wishes.' "[65] Given the EU's historical emphasis on personal privacy, the EU most likely fashioned the Directive in order to protect individuals through both opt-in and opt-out measures.

Although experts disagree about the conflicting terminologies, they mutually agree that the 2009 ePrivacy Directive does not answer the question of how the user's consent will be obtained.[66] The 2009 ePrivacy Directive states that "the user's consent to processing may be expressed using the appropriate settings of a browser or other application."[67] A user would express consent through the settings on his browser so that it reflects his individual privacy preferences.[68] However, less sophisticated users are less likely to be aware of their ability to change the default settings chosen by the manufacturer of the Internet browser,[69] which is usually set to a low level of privacy protection.[70] This assertion is supported by the Data Protection Working Party (Working Party), an independent advisory body on data protection and privacy created by Article 29 of the EU Directive.[71] The Working Party issued an opinion stating that "[i]t is a fallacy to deem that on a general basis data subject inaction . . . provides a clear and unambiguous indication of his/her wishes."[72] The question of browser setting choices thus

---

Amended by Directive 2009/136/EC), *in* ELEVENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW 49, 62 (2010).

[63] *Id.*

[64] *Id.* at 63.

[65] Lanois, *supra* note 8, at 17 (quoting Council Directive 95/46, *supra* note 48, art. 2).

[66] *See, e.g.*, Gilbert, *supra* note 62, at 62–63 (arguing that the user's expression of consent through an Internet browser causes confusion).

[67] 2009 O.J. (L 337) 20 at (66).

[68] *See* Lanois, *supra* note 8, at 17 ("[W]hen the user has set his or her browser settings to reject cookies, then such a privacy setting would be sufficient to indicate his or her refusal to allow the content provider to store information or gain access to information stored on the computer.").

[69] *See* Gilbert, *supra* note 62, at 62–63 (noting that less sophisticated Internet users choose the setting determined by the manufacturer of the product).

[70] *See* Lanois, *supra* note 8, at 20 (stating that three major Internet browsers have default settings allowing the free flow of cookies, technology used to track users as they browse the Internet).

[71] Council Directive 95/46, art. 29, 1995 O.J. (L 281).

[72] Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioral*

brings up the question of consent or, more specifically, the extent to which users can consent when they are not aware of what they are consenting to.[73]

Despite these updates, however, EU legislation remains obsolete.[74] In 2010, the European Commission (EC) had experts draft a report on the future of cloud computing in the European Union.[75] The report noted that the current legislation is vague and not inclusive of developments in cloud computing technology.[76] The findings of the report reflect the legal recommendations made by the European Network and Information Security Agency (ENISA) in their 2009 report, which included a detailed risk assessment of cloud security.[77] The ENISA Report called for clarification of certain terms as well as the re-examination of concepts such as "transferring data" in light of new technological developments since the 2009 ePrivacy Directive was drafted.[78]

The USA Patriot Act of 2001[79] (Patriot Act) presents further barriers to widespread European acceptance of the cloud.[80] The Patriot Act "expands law enforcement's surveillance and investigative powers and grants the U.S. government the right to demand data on the grounds of homeland security."[81] As a result of the broad right of surveillance granted in the Patriot Act, European customers fear that the U.S. government could gain access to sensitive information in the course of an investigation.[82] In addition, the EU

Advertising, WP 171, at 14 (June 22, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

[73] Lanois, supra note 8, at 17 ("[C]an informed consent be validly implied if the user has not changed the browser's default settings that are set to allow all cookies?").

[74] *See id.* at 31 (contending "there is still some uncertainty regarding the extent of the rules within a cloud computing environment" within the European Union).

[75] *See* Lutz Schubert, *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*, EUROPEAN COMMISSION, *available at* http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[76] *See id.* at 46 ("[T]here are plenty unsolved legalistic issues yet to be addressed, in particular related to the location of data and / or code.").

[77] Daniele Catteddu & Giles Hogben, *Cloud Computing: Benefits, Risks, and Recommendations for Internet Security*, EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY [hereinafter ENISA Report], *available at* http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[78] *Id.* at 84–85 (calling for clarification of terms such as "Joint Controller," research about the effect of data transfers to countries that do not meet the security threshold set by the EU Directive, etc.).

[79] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.).

[80] *See* Denny, *supra* note 6, at 239 (noting that European companies are hesitant to have their data stored on computers in the U.S. government would be able to easily access that data).

[81] Lanois, *supra* note 8, at 24.

[82] *Id.*

Directive puts "stringent standards on the collection of electronic data by the government and by any other entity."[83] The EU Directive allows information to be transferred outside of the EU only if the receiving country ensures an "adequate" level of protection—the United States is not deemed to be one of these countries.[84]

In order to promote European development of cloud-based services, the U.S. Department of Commerce and the European Commission developed the International Safe Harbor Certification program,[85] which provides a framework of data protection principles.[86] The goal of the Safe Harbor framework is to "permit the transfer of personal data from the EU to the U.S. while assuring an 'adequate' privacy protection overseas."[87] The safe harbor framework allows U.S. organizations to "self-certify" that their standards comply with the EU Directive's standard of an "adequate level of protection"[88] and also adhere to the Safe Harbor principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.[89] Despite these measures, however, international companies are still hesitant to enter the EU cloud computing market.[90]

B. United States

In contrast to the overarching regulations of the EU, privacy legislation development in the U.S. "has been very fragmented and sector-specific."[91] In addition, many impediments hinder the judicial and legislative development of privacy protections in the context of cloud computing.

---

[83] Denny, *supra* note 6, at 239.

[84] Lanois, *supra* note 8, at 27.

[85] U.S.–E.U. Safe Harbor Framework, http://export.gov/safeharbor/eu/eg_main_018365.asp (last updated Mar. 31, 2011).

[86] David Satola & Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 WM. MITCHELL L. REV. 1745, 1765 (2011).

[87] Lanois, *supra* note 8, at 29.

[88] *Id.*

[89] Shick, *supra* note 47, at 185.

[90] *See* O'Brien, *supra* note 34 (noting that it is costly and time-consuming to prepare EU-mandated service agreements between data processors and cloud computing providers located in countries that have not been approved by the EU to provide cloud computing services).

[91] Symposium, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1, 16 (2007).

1. The Judicial Perspective

The Fourth Amendment of the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, paper, and effects, against unreasonable searches and seizures," and provides that this right "shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[92] The Fourth Amendment is therefore designed to protect against the search of private documents such as a person's diary, personal letters, and other property.[93] The emergence of cloud computing has led to questions about the extent of Fourth Amendment protections regarding individual privacy in the framework of new technologies.[94]

Cloud service users often depend on cloud providers to provide sufficient security for their information.[95] However, courts have held that the Fourth Amendment doctrine precludes an expectation of privacy when information is provided to a third party.[96] The reason for this conclusion is the third-party doctrine, the idea that people have no expectation of privacy in the information communicated with a third party.[97] The third-party doctrine was applied in *Wilson v. Moreau*, in which the court held that a public library employee did not have a reasonable expectation of privacy because "[t]he library was an open and public work environment, the computers were available for public use, the stored documents were accessible to other computer users, and whatever e-mails that were stored in the system had been disseminated or received over the shared network."[98] This case and others applying the Fourth Amendment suggest "that courts are unlikely to enhance privacy protections for cloud computing users."[99] The lack of Fourth Amendment protections in this context may result in "online service providers [being] compelled to reveal their customers' private documents with a mere subpoena."[100] Thus, although the third party doctrine is not the main reason for the lack of privacy online, its application by the courts "is

---

[92] U.S. CONST. amend. IV.

[93] Soghoian, *supra* note 4, at 390.

[94] Kattan, *supra* note 19, at 623.

[95] *See* Soghoian, *supra* note 4, at 375 (noting the extent of data, such as bank account information, that is stored on web-based services).

[96] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose . . . .").

[97] *Id.* at 442.

[98] Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (D.R.I. 2006).

[99] Robison, *supra* note 9, at 1232.

[100] Soghoian, *supra* note 4, at 391.

certainly the current tool of choice for the government's evisceration of the Fourth Amendment . . . ."[101]

2. The Electronic Communications Privacy Act and the Stored Communication Act

The Electronic Communications Privacy Act (ECPA) was enacted by Congress in 1986.[102] The ECPA was designed to increase privacy protection in the face of developing technologies by requiring law enforcement to adhere to a higher standard when attempting to access electronic data.[103] Among other provisions, the ECPA prohibits, with some exceptions, attempted or actual interceptions and disclosures of "any wire, oral, or electronic communication."[104] However, the ambiguous definition of "intercept" depends on an archaic interpretation of "communication."[105] Intercept is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[106] This definition should apply to data stored in the cloud, but "courts have struggled to clarify" the meaning of communication.[107] For instance, in *United States v. Ropp*, the court dismissed charges against an employer who attempted to eavesdrop on the computer activities of one of his employees using KeyKatcher, a program that records the electronic signals generated by depressing keys on a keyboard.[108] The court based its decision on the fact that this interception did not fall under the ECPA's definition of "electronic communication" because it was stored on local computer hardware, the computer's Central Processing Unit, and was never transmitted through a network.[109] This ruling was based on the traditional model of computing in which users must actively connect to the Internet, and are only connected for short periods of time.[110] However, in the world of cloud computing, where internet users are always connected, this interpretation of "electronic communication" is no

---

[101] *Id.*
[102] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522 (2006)).
[103] Martin, *supra* note 24, at 305.
[104] 18 U.S.C. § 2511 (2006).
[105] Martin, *supra* note 24, at 305.
[106] 18 U.S.C. § 2510(4) (2006).
[107] Martin, *supra* note 24, at 305.
[108] United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004).
[109] *Id.* at 837–38.
[110] Martin, *supra* note 24, at 306.

longer valid.[111] The problem of interpretation here may also cause confusion when applying other parts of the ECPA.

The Stored Communication Act (SCA) was enacted by Congress as part of the ECPA to protect information kept in electronic storage.[112] Congress sought to regulate two primary uses of computer networks: (1) electronic communication service (ECS), which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[113] and (2) remote computing services (RCS), which are "intended to provide outsourced computer processing and data storage."[114] A remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[115]

The SCA offers different protections depending on the characterization of the service (ECS or RCS).[116] Data stored with an RCS "receives fewer privacy protections than communications held by an ECS."[117] Most cloud computing services can fall within the definition of either category, which could potentially lead to confusion in applying the SCA.[118] For messages stored in an ECS for 180 days or less, the SCA requires that law enforcement obtain a search warrant.[119] If the message has been stored for 180 days, law enforcement can gain access using the lower RCS threshold.[120] However, when it comes to nongovernmental entities users may have less privacy control over their personal identifying information such as name, physical and e-mail addresses, and IP address.[121] A service provider "may divulge a record or other information pertaining to a subscriber to or customer of such service to any person other than a governmental entity."[122] The government can also compel service providers to disclose personal information through an administrative subpoena.[123]

---

[111] *See id.* (noting that broadband Internet connections in today's society "are always on, always connected").
[112] 18 U.S.C. §§ 2701–2712 (2006).
[113] *Id.* § 2510(15).
[114] Robison, *supra* note 9, at 1205.
[115] 18 U.S.C. § 2711(2) (2006).
[116] Kattan, *supra* note 19, at 631.
[117] Robison, *supra* note 9, at 1208.
[118] Martin, *supra* note 24, at 307.
[119] 18 U.S.C. § 2703(a) (2006).
[120] *Id.* § 2703(b).
[121] Robison, *supra* note 9, at 1208.
[122] 18 U.S.C. § 2702(c)(6) (2006).
[123] *Id.* § 2703(c)(2).

Quon v. Arch Wireless Operating Co. is one example of the difficulty courts face in determining whether a service is an ECS or RCS.[124] In Quon, the Ninth Circuit held that a text-messaging service was an ECS despite the fact that the service provider had archived the messages and offered remote messaging services.[125] When determining that the service was an ECS, the court relied on the legislative history of the SCA.[126] Unfortunately, this legislative history dated back to 1986, and the law was formed based on the definitions of technology at that time.[127] The court's approach thus relies on definitions based on obsolete technology in an environment where these distinctions no longer matter.[128]

These issues with interpretation of the SCA demonstrate that it "fails to provide a clear framework for understanding whether a user has a reasonable expectation of privacy in his communications stored in the cloud."[129] Therefore, although the ECPA does provide certain privacy protections against law enforcement,[130] it has not caught up to the advancements introduced by cloud computing.[131]

3. The Computer Fraud and Abuse Act

In 1986, Congress passed the Computer Fraud and Abuse Act (CFAA) in order to address computer hacking,[132] but it has been broadened to include both civil and private rights of action for breaches of the Act.[133] The CFAA prohibits

---

[124] Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).
[125] *Id.* at 902.
[126] *Id.* at 901.
[127] *Id.*
[128] Martin, *supra* note 24, at 307.
[129] Kattan, *supra* note 19, at 645.
[130] *See, e.g.*, 18 U.S.C. § 2515 (2006) (prohibiting law enforcement from the use of illegally intercepted wire or oral communication); 18 U.S.C. §§ 2516, 2518 (requiring that law enforcement follow a detailed process to obtain authorization to intercept communication).
[131] Kattan, *supra* note 19, at 648 ("In 1986, when ECPA was passed, the Internet consisted of a few thousand computers . . . . There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades." (quoting *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 2 (2010) (statement of Edward W. Felten, Professor of Computer Science and Public Affairs at Princeton University))).
[132] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 (2006)).
[133] Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 429 (2009).

(1) the unauthorized access and disclosure of data that "could be used to the injury of the United States,"
(2) the unauthorized acquisition of data from financial institutions, U.S. agencies, or a private computer used in interstate commerce,
(3) unauthorized access to a U.S. department or agency computer,
(4) unauthorized access to a protected computer with knowledge and the intent to defraud and obtain something of value
(5) the intentional damage of a protected computer, or an intentional transmission of a program that causes damage to a protected computer
(6) the intentional trafficking of passwords of protected computers with an intent to defraud, or
(7) the threat to damage a protected compute with the intent to extort something of value.[134]

Although the CFAA "seems to create a powerful deterrent to most computer crime," it lacks the force to be an effective deterrent to cybercrime.[135] For instance, felony penalties are only triggered when the damage exceeds $5,000 within a one-year period.[136] However, actual damage is often "difficult to ascertain or quantify," and programs that are installed on one date may not cause harm until much later.[137] Thus, it would seem that the CFAA is yet another privacy law that needs to be updated to conform to the current cloud computing framework.

C. China

Like the United States, China has passed some sector-specific laws,[138] but cloud computing has not been directly addressed by Chinese law.[139] However, there are some sector-specific laws that could still apply to the

[134] 18 U.S.C. § 1030(a) (2006).
[135] Martin, *supra* note 24, at 308.
[136] 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2006).
[137] Martin, *supra* note 24, at 308.
[138] Donald C. Dowling, *International Data Protection and Privacy Law*, PRACTISING LAW INSTITUTE (Aug. 2009), http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.
[139] Sarah Xuan, *Legal Issues Associated with Cloud Computing in China*, HG.ORG (Nov. 23, 2010), http://www.hg.org/article.asp?id=20501.

cloud computing structure.[140] First, Article 12 of the Ministry of Information Industry's Administration of Internet Electronic Messaging Services Provisions states "[e]lectronic messaging service providers shall maintain the confidentiality of the personal information concerning the online subscribers and may not disclose the same to third parties without the subscribers' consent . . . ."[141] Second, Article 7 of the Computer Information Network and Internet Security, Protection and Management Regulations states "[t]he freedom and privacy of network users is protected by law," adding "[n]o unit or individual may, in violation of these regulations, use the Internet to violate the freedom and privacy of network users."[142] This regulation could be applied to cloud computing to protect against Internet hackers and viruses. Another provision that could protect against hackers is Article 18 of the Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China, which states:

> Internet users are forbidden from entering certain computer systems without permission and illegally changing [third party] information; distributing malicious information, giving out information in other people's names and violating others' privacy through networks; developing and spreading computer viruses[,] and engaging in other activities in violation of legitimate rights and interests of networks and individuals.[143]

Another potentially applicable regulation is the Interim Administrative Measures on Internet-based Transactions of Goods and Related Services (Interim Measures), which focuses on business-to-consumer (B2C), business-to-business (B2B) and consumer-to-consumer (C2C) activities.[144]

---

[140] *Id.*

[141] Administration of Internet Electronic Messaging Services Provisions (promulgated by the Ministry of Industry and Info. Tech., effective Oct. 8, 2000), http://www.chinesewalker.cn/2009/08/15/ministry-of-information-industry-administration-of-internet-electronic-messaging-services-provisions/.

[142] Computer Information Network and Internet Security, Protection and Management Regulations (promulgated by the Ministry of Pub. Sec., effective Dec. 30, 1997), http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html.

[143] Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China (promulgated by the Information Computerization Leaders Group of the State Council, effective Feb. 13, 1998), http://www.wipo.int/wipolex/en/details.jsp?id=6562.

[144] Interim Measures for the Trading of Commodities and Services through the Internet (promulgated by the State Administration for Industry and Commerce, May 31, 2010,

Although the Interim Measures are aimed at regulating e-commerce sites such as Taobao.com(C2C) and alibaba.com(B2B),[145] its existence may indicate a trend toward regulation and increased consumer advocacy in China. Thus, Chinese consumers may have their privacy protected against private corporations, but enjoy no such protection against the Chinese government.

In the absence of clear legal guidelines specifically addressing cloud computing, the context in which the Internet and consumer privacy has developed should be analyzed. In 2009, the International Data Corporation (IDC) estimated that only four percent of Chinese businesses were using cloud-based services.[146] This is, in part, because China's large state-owned businesses want to maintain control of IT assets, and are, therefore, suspicious of third-party services, such as cloud computing.[147] However, although its usage of web-based technology "lags badly," the fact that China has the world's largest population of Internet users,[148] and increasing Internet sophistication may play a factor in the development of cloud computing in China's business sector.

Despite most Internet users' suspicion of the cloud, cloud computing development "benefits from a favo[ ]rable policy environment in China."[149] China's Ministry of Industry and Information Technology (MIIT) has focused on cloud computing as a "key project" in China's technological development.[150] In 2010, the MIIT chose Beijing, Shanghai, Shenzhen, Hangzhou, and Wuxi to lead the way in cloud computing and development, and up to two trillion yuan in government funds are being devoted to telecommunications infrastructure investment.[151] China's city governments

---

effective July 1, 2010), http://lawprofessors.typepad.com/files/interim-measures-for-supervision-and-management-of-internet-information-service-market-ito-trans-2.pdf.

[145] Steven Chow, *First Ecommerce Regulation Introduced in China*, CHINA ONLINE MARKETING (June 1, 2010), http://www.china-online-marketing.com/news/laws-regulations/first-ecommerce-regulation-introduced-in-china/.

[146] Wayne Arnold, *Regulations and Security Concerns Hinder Asia's Move to Cloud Computing*, N.Y. TIMES, Oct. 12, 2010, at B8.

[147] *Id.*

[148] Christina Larson, *The Man Behind Cloud Valley*, TECH. REV. (Oct. 24, 2011), http://www.technologyreview.com/business/38726/?p1=BI.

[149] Andrew McGinty, *The Hazy Cloud – Legal Challenges for Delivering Cloud Computing in China*, HOGAN LOVELLS, http://ehoganlovells.com/rv/ff0001f56ad18fc97abed201ea4aaf4ecab5ac52/p=6 (last visited Dec. 15, 2011).

[150] *Gov't Investment in Cloud Computing Essential, Says Microsoft*, XINHUA (June 18, 2010), http://www.china.org.cn/business/2011-06/18/content_22810819.htm; *see also* Tony Zhu, *China's Cloud Computing Market Could Reach RMB 1 tln by 2013*, BUS. CHINA (Apr. 12, 2011), http://en.21cbh.com/HTML/2011-4-12/4OMjMyXzIwOTg4OA.html (stating that the MIIT has earmarked 5 Chinese cities to pilot cloud computing development).

[151] Henry Acland, *China Focus: The Virtualization of a Nation, Cloud Computing in China*

also have announced plans for significant investment in cloud computing development.[152] In addition, the Chinese government, recognizing that cloud computing, as a developing industry, is lacking in regulation, has also pledged to develop more cloud regulations in the future.[153]

The Chinese government's eager endorsement of cloud computing may cause conflict with its privacy policy, which is widely recognized as the world's strictest in regards to internet freedom.[154] Although China's Constitution provides for freedom of speech,[155] China has zealously practiced internet censorship in the name of national security.[156] In fact, China has enacted certain laws that permit the Chinese government to attain this private information in the name of state security.[157] These laws prohibit information that endangers state security, deteriorates to the state's honor, causes ethnic oppression, disseminates rumors that disrupt social stability, spreads pornography, undermines state religious policy, or "preaches the teachings of evil cults."[158] The terms of these regulations are "needlessly vague," which results in over-censoring since users lack adequate guidelines as to what is or is not appropriate.[159] While Chinese regulations signal a trend toward consumer protection against corporations, no protection is offered against government intrusion. This discrepancy could hinder the development of cloud computing in China, especially as its increasingly Internet-savvy population moves its data to the cloud.

Takes Hold, XINHUA (June 29, 2011), http://news.xinhuanet.com/english2010/china/2011-06/29/c_13956822.htm.

[152] Shervin Bakhtiari, *Cloud Computing in China – The Greatest Hurdle?*, BUS. CLOUD NEWS (Oct. 17, 2011), http://www.businesscloudnews.com/platform-as-a-service/604-can-cloud-computing-prosper-in-china.html.

[153] *MIIT: To develop planning standards of cloud computing*, C114 (July 21, 2011, 2:10 PM), http://www.cn-c114.net/575/a630404.html.

[154] *See, e.g.*, Joseph Kahn, *China Says Web Control Follows the West's Lead*, N.Y. TIMES, Feb. 15, 2006, at A6 ("China operates a vast and technologically sophisticated firewall to protect the ruling Communist Party against what it views as Web-based threats to its authority.").

[155] Constitution of the People's Republic of China, Dec. 4, 1982, art. 35 (China).

[156] *See* Jessica E. Bauml, *It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship*, 63 FED. COMM. L.J. 697, 707–08 (2011) (arguing that although China "contends that censorship is necessary to promote the nation's stability and maintain security by avoiding political upheaval," its "censorship laws are on the extreme end of the spectrum").

[157] State Security Law of the People's Republic of China (promulgated Order No. 68 of the President of the People's Republic of China, effective Feb. 22, 1993), http://www.china.org.cn/english/government/207480.htm.

[158] Measures for Managing Internet Information Services (promulgated by Decree No. 292 of the State Council of the People's Republic of China, effective Sept. 25, 2000), http://www.chiaculture.org/library/2008-02/06/content_23369.htm.

[159] Bauml, *supra* note 156, at 705.

IV. CORPORATE COMPLICITY

Cloud users may also be subject to government intrusion via the cloud providers who protect their private data. For instance, China's censorship laws impose obligations on foreign internet content providers, such as Yahoo and Microsoft.[160] In 2006, the Chinese government succeeded in forcing Microsoft to shut down the blog of an outspoken government critic, Zhao Jing.[161] In 2005, Chinese journalist Shi Tao was sentenced to ten years in prison for sending "state secrets" to foreign websites through his Yahoo account.[162] The arrest was made possible by Yahoo's offices, which handed over the information that was ultimately used to identify the account holder.[163] Due to the Chinese government's strict censorship policy, cloud computing corporations operating in China may have to compromise their customers' privacy in order to satisfy the government's demands.

Cloud computing consumers in the U.S. and the EU may also be affected by such government-mandated corporate intrusion, though it may not be as overt as the cases in China. Although American companies profess a devotion to their customers' privacy to the press,[164] critics argue that the only privacy interest actually being protected is the companies' "own collection and commercial use of customer data and the extent to which they share it with other companies."[165] Customers are therefore not protected from intrusion by the government,[166] and "firms are now regularly compelled to modify their products in order to facilitate the government's interest in surveillance and search."[167] For example, a U.S. statute requires that both ECS and RCS providers must notify authorities upon learning of the presence of child pornography on their servers.[168] Cloud providers are therefore obligated to "review content that has been flagged by their users or

---

[160] *Id.*

[161] *The Long March to Privacy*, ECONOMIST (Jan. 12, 2006), http://www.economist.com/node/5389362.

[162] *US Rebukes Yahoo over China Case*, BBC NEWS (Nov. 6, 2007, 7:11 PM), http://news.bbc.co.uk/2/hi/technology/7081458.stm.

[163] *The Long March to Privacy*, *supra* note 161.

[164] *See* Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 191–92 (noting that companies such as Verizon, Google, and Microsoft are committed to protecting their customers' privacy).

[165] *Id.* at 193.

[166] *See id.* ("Few companies effectively protect their customers' data from intrusive government searches.").

[167] Soghoian, *supra* note 4, at 400.

[168] 18 U.S.C. § 2258A (2006).

other third parties."[169] They are not, however, obligated to seek out such materials, although several ISPs have chosen to do so.[170] Critics argue that this approach could lead to questionable information gathering because "once a technical infrastructure has been designed and deployed, service providers are not in a position to limit the extent to which they can be compelled to use it."[171]

Adopting a zero data retention policy is one way that cloud computing providers could protect costumers' privacy. When no information about the customer is stored, no information is available to the government. Despite the fact that the costs of keeping data are increasingly cheap, the costs incurred by cloud providers through lawsuits and data breaches may provide a financial incentive for corporations to delete data.[172] Although some IPSs in Sweden have enacted zero data retention policies in response to customer demands, none of the major American ISPs or telecommunications carriers have done so.[173] As a result of the adoption of the zero data retention policies in Sweden, the head of the Swedish Police's National IT crime unit noted that it has become "harder for the police to track down criminals carrying out serious crimes."[174] This response could echo the American government's likely argument that if they were not able to force cloud providers to reveal customers' information, it would be much more difficult to catch pedophiles and terrorists.

Cloud computing has made government intrusion cheaper and easier to obtain than ever.[175] A zero data retention policy may be available to corporations, but they are unlikely to adopt that policy because of business models such as Google's, which "mines" the data of its users to provide targeted advertisements and generate revenue for itself.[176] Thus, what is likely the most effective way to protect consumer privacy is through an overarching legal structure such as that of the EU.

---

[169] Soghoian, *supra* note 164, at 202.

[170] *See, e.g.*, United States v. Richardson, 607 F.3d 357, 362–63 (4th Cir. 2010) (noting that AOL developed a program to scan its customers' email attachments of child pornography).

[171] Soghoian, *supra* note 164, at 203.

[172] *Id.* at 209.

[173] *Id.* at 214.

[174] Enigmax, *Police Say Anti-Piracy Law Makes Catching Criminals Harder*, TORRENTFREAK (May 17, 2010), http://torrentfreak.com/police-say-anti-piracy-law-makes-catching-criminals-harder-100517/.

[175] *See* Soghoian, *supra* note 4, at 398 ("A move to encrypted cloud-based services will likely lead to a significant reduction in the ease with which law enforcement agents can obtain the private files of suspects.").

[176] *Id.* at 396.

V. INTERNATIONAL SOLUTIONS

A. Barriers to International Cooperation

Cultural standards may affect each region's approach to privacy legislation. For example, in the U.S., "Americans have been less likely than Europeans to turn to the government to regulate private enterprise, instead relying on the market or new technologies to address public concerns about commercial activity."[177] In contrast, the EU's policy of strict protection of personal privacy is shaped by the brutal events of World War II.[178] In China, less concern about personal privacy may be a result of the collectivist society,[179] which calls for the sacrifice of personal privacy to benefit group efforts.[180] However, although privacy has not traditionally been valued in China, the concept of privacy may be gaining currency as Western technology and attitudes continue to infiltrate Chinese society.[181] The changing attitudes of the Chinese may be useful in drafting a cloud computing privacy policy that could be applied globally.

The cultural discrepancies between these three diverse regions may be offset by the integration of the U.S., EU, and Chinese economies, which is reflected in areas such as "the number of corporate offices in each other's jurisdictions and the significant personal data flows between the two economies."[182] Another important economic factor that may affect international cooperation in the area of cloud computing privacy policy is the "entangled and dependent" relationship between the U.S. and China.[183]

---

[177] Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 471 (2000).

[178] *See, e.g.*, Marsha C. Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 441 (noting that EU policy "is the culmination of over fifty years of Western European devotion to recognizing, maintaining, restoring, and ensuring personal privacy" following the "barbarous acts" of World War II); Ryan Moshell, Comment, *. . . And Then There Was One: The Outlook for a Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 359 ("[A] European Union (EU) data-protection regime vigorously defends the privacy of an individual's personal information from both the government and the private sector, largely as a result of the region's grisly past.").

[179] Yang Wang et al., *Who Is Concerned About What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites*, *in* TRUST AND TRUSTWORTHY COMPUTING 146, 152 (Jonathan McCune ed., 2011).

[180] *See* David Brooks, *Harmony and the Dream*, N.Y. TIMES, Aug. 12, 2008, at A21.

[181] *The Long March to Privacy*, *supra* note 161.

[182] Satola & Judy, *supra* note 86, at 1768.

[183] Bauml, *supra* note 156, at 716 (noting that "China holds about $800 billion of America's debt, while the United States is China's most important market for its goods").

Although the relationship is complicated and strained,[184] the interconnectedness of these two countries' economies may provide incentives for both the U.S. and China to maintain a good relationship.

B. Proposals to Ensure Privacy in Cloud Computing

In order to address the issues of privacy in the cloud, several industry, nonprofit, and government-sponsored groups have released proposals that should be considered in drafting a policy about this topic.

One example of such a proposal is the Communication, subtitled "A comprehensive approach on personal data protection in the European Union" (EU Communication), issued by the European Commission to the EU Parliament and the Council in November 2010.[185] The EU Communication addresses the effects of cloud computing on privacy law, noting that changes will have to be made to legislation based on the international nature of data stored in the cloud.[186] In addition, the EU Communication maintains the privacy focus of previous legislation but emphasizes that changes such as increased transparency to consumers need to be made in order to ensure personal privacy.[187]

An alternative proposal is Microsoft's Cloud Computing Advancement Act, a legislative and industry initiative designed to "promote innovation, protect consumers, and provide the [E]xecutive [B]ranch with the new tools needed for a new technology era."[188] Noting that the ECPA was enacted before the invention and utilization of current cloud technologies, the proposal advocates for an update to the ECPA to fill in the legal gaps in the current statute.[189] The proposal also calls for bilateral and multi-lateral discussions between countries, with Congress taking the lead in the U.S. in helping "build consensus with other parliamentary holders."[190]

---

[184] Matt Spetalnick & Doug Palmer, *Obama to China: Behave Like a "Grown Up,"* REUTERS (Nov. 14, 2011, 9:23 AM), *available at* http://www.reuters.com/article/2011/11/14/us-apec-idUSTRE7AB12920111114?feedType=RSS&feedName=topNews&rpc=71.

[185] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive Approach on Personal Data Protection in the European Union*, COM [2010] 609 final (Nov. 4, 2010).

[186] *See id.* at 4 ("Several stakeholders highlighted that the increased outsourcing of processing, very often outside the EU, raises several problems in relation to the law applicable to the processing and the allocation of associated responsibility.").

[187] *Id.* at 6.

[188] Brad Smith, General Counsel, Microsoft Corporation, Address at the Brookings Institute Policy Forum, 19 (Jan. 20, 2010).

[189] *Id.* at 21–22.

[190] *Id.* at 30.

In terms of practical considerations, the first step for nations concerned about the privacy implications of cloud computing is to agree on a uniform definition of cloud computing. This definition should be updated with regularity so that legislation can keep up with the rapid developments that are to come as the cloud computing industry develops. Only with regular assessments about the applicability of existing law can cloud users be adequately protected.

Along with regular updates, international actors should emphasize personal privacy as a focus of legislation regarding cloud computing. The EU should build on its current policy of stringent privacy protection while striving to update its obsolete legislation. The 2009 ePrivacy Directive should be updated, taking into consideration the recommendations of proposals, such as the EU Communication. New policy should also seek to change the attitudes of European cloud users so that they feel more secure in storing their information in the cloud.

In the U.S., Congress should eliminate the SCA's ECS and RCS categories and the distinction between how these two categories are treated because they are outdated and confusing for courts to apply. Furthermore, the ECPA should undergo a comprehensive overhaul that will result in a final product that reflects developing technologies and the privacy implications that go along with those developments. Punishments for violations under the ECPA and the CFAA should, also, be reevaluated and made more severe; the existing punishment structure has not proven to be a clear deterrent against malicious online activity.

While arguing that China should adopt a privacy policy that promises privacy from both the government and private corporations is easy, expecting the Chinese government to loosen its censorship in the face of new technologies is unrealistic. American privacy law has had over two hundred years to develop, while China is still a maturing nation that has not had the time to develop their privacy framework.[191] Thus, the best step may be to allow privacy protection in China to develop alongside cloud computing, letting market forces govern how privacy legislation is shaped. By hesitating to block Google completely following a showing of support by Chinese citizens, the Chinese government has already shown that it is cognizant of foreign cloud providers as well as the attitude of its citizens.[192]

Although government participation is important, cloud providers must protect the rights of its customers against the government and against themselves. To that end, cloud providers should adopt policies that limit the

---

[191] Bauml, *supra* note 156, at 725–26.
[192] *Id.* at 728–29.

amount of data that they can retain. Although a zero retention policy is likely unrealistic, a policy that strikes a balance between government interests and personal privacy would prove beneficial to all parties.

VI. CONCLUSION

As more and more of our information is moved to the cloud, sources of intrusion increase: hackers, corporate data mining, and government surveillance. Information that was once only available on one computer is now spread out on worldwide servers, bringing questions of jurisdiction and data safety.

The legislative framework in the U.S., EU, and China are not equipped to deal with the new technology presented by cloud computing. While legislation in the U.S. and EU are obsolete in the context of privacy in modern cloud computing, the Chinese government has no provisions for privacy against online government intrusion. Corporations, also, play a role in assisting governments in violating the privacy of its citizens.

In order to update cloud computing legislation with modern notions about personal privacy, cooperation needs to happen at the international level. Following international discussions on the definitions and implications of cloud computing, national legislators should implement laws that update modern Internet personal privacy, addressing issues such as increased punishment for violations and outdated definitions.