
Timothy D Martin, Southern Methodist University
Introduction

I. How Cloud Computing Works
   A. Software-as-a-Service: Familiar Places on the Web
   B. Platform-as-a-Service: Databases, Large-Scale Storage, and Web Servers
   C. Infrastructure-as-a-Service: Large-Scale Application Deployment in the Cloud
   D. Advantages and Benefits of Cloud Computing

II. Barriers to Confidence in the Cloud
   A. Technological Barriers to Acceptance of Cloud Computing
   B. Ownership and Control Barriers to Acceptance of Cloud Computing
   C. The Fourth Amendment and the Government’s Access to Data in the Cloud
   D. Inadequate Statutory Law: The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act

III. Proposals to Enhance Confidence in the Cloud
   A. Microsoft and the Cloud Computing Advancement Act
   B. The Center for Democracy & Technology and Digital Search & Seizure
   C. IBM and the Open Cloud Manifesto
   D. The European Union and the ENISA Report
   E. Beyond the Current Proposals: A Common-Sense Approach to Privacy, Security, and Ownership in the Cloud

Conclusion

* J.D. Candidate, SMU Dedman School of Law, 2011. tmartin@smu.edu
Introduction

The thing that hath been, it is that which shall be; and that which is done is that which shall be done: and there is no new thing under the sun. Is there any thing whereof it may be said, See, this is new? it hath been already of old time, which was before us.¹

Imagine that you have just passed the bar examination and want to start a new solo practice. Or perhaps you are an entrepreneur who wants to start a new business. In either case, one of your foremost concerns will be how to deal with computer hardware and software, networking, and online access.² Because you have limited resources, you might turn to cloud computing—software and computing power you access online—as a cost-effective solution for your information technology needs.³ But cloud computing raises questions of functionality, security, privacy, ethics, enforcement, and ownership of the electronic data that will fuel your efforts.⁴ And though cloud computing involves new technology, the challenges it presents in the areas of security and confidentiality are ancient.⁵ This paper argues that Congress and other authorities need to act soon to unify the law, clarify the property boundaries of data used in cloud

---

¹ Ecclesiastes 1:9–10 (King James).
computing, and help establish procedural and ethical standards for security and confidentiality in cloud computing.

Cloud computing allows individuals and businesses to purchase and use sophisticated technology services over the Internet on an as-needed basis. These services might include anything from e-mail and word processing to software development and complex data center operations. Cloud computing is a cost-effective alternative to buying and maintaining expensive and complicated computer hardware and software, but it is not really new. As long as fifty years ago, organizations could connect widely-dispersed terminals to a mainframe computer. So cloud computing is nothing more than the application of old principles using new technology. Part I of this paper discusses the various aspects of cloud computing and the range of cloud computing applications.

Though adoption of cloud computing is clearly on the rise, barriers to public acceptance exist—mainly concerning the security and confidentiality of data. Part II discusses some of the risks associated with cloud computing including how current U.S. law deals with or contributes to those risks. Many of the risks have familiar-sounding names such as spam, viruses, worms,

6 Kirsner, supra note 2, at ¶ 2.
7 Id.
8 Id.
9 Kennedy, supra note 3, at ¶ 1.
10 Id. As Dell found out when it attempted to trademark “CLOUD COMPUTING,” the term has become generic and cloud services have become almost ubiquitous. See USPTO Office Action (Aug. 12, 2008) for trademark application serial no. 77/139082 (rejecting Dell’s trademark application for CLOUD COMPUTING based on descriptiveness and genericness).
Trojan horses, logic bombs, sniffers, denial-of-service attacks, web bots, and spiders. But the lack of a clear body of law defining and regulating law enforcement’s access to electronic data and ability to prosecute related crimes creates other risks and erodes confidence in cloud computing.

In order to spur confidence in cloud computing, industry leaders recently proposed new legislation, standards, and governing principles. Part III discusses these proposals and their interaction with federal law. Microsoft’s proposed legislation, dubbed the Cloud Computing Advancement Act, calls for Congress to revamp federal laws related to online privacy, security, and computer crime. The Center for Democracy & Technology previously proposed similar changes to enhance constitutional privacy protection. And the Open Cloud Manifesto, put forth by a consortium of industry leaders including IBM, advocates an “open cloud” through more standardization and collaboration.

But these proposals contain gaps that expose issues that could continue to threaten the vitality and development of the cloud. Part III also discusses these additional problems and proposes a more comprehensive solution that combines legislation, regulatory oversight, and industry

---

14 See James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 ALB. L.J. SCI. & TECH. 65, 67-68 (1997) (describing the need to find a proper balance between the needs of law enforcement and the privacy of individuals’ online data).
16 See generally Smith Whitepaper, supra note 15.
collaboration. Ownership of some kinds of electronic data—in particular, the data stream users create as they interact with web-based applications—would still be poorly defined under the industry proposals. That would continue to present problems because of the dispersion of data across many physical locations. Any solution needs to incorporate guarantees that data owners would be able to gain control of their data in a usable form should their service providers become inoperable.\(^\text{19}\) Another aspect of ownership that would remain poorly defined is whether users of cloud services retain ownership of their online identities (such as a seller-rating on eBay) and control over their desktop computers (whether license agreements allow users to employ third-party productivity software).\(^\text{20}\)

Further, the lack of any uniform ethical guidance might prevent certain kinds of professionals from willingly using cloud services.\(^\text{21}\) This is likely to grow into an even larger issue over time as technology erases the line between online content (data stored remotely) and offline content (data stored on a user’s computer).\(^\text{22}\) The Microsoft, Center for Democracy & Technology, and IBM proposals address some of these issues in a general way through industry standardization and openness. But promises of technological cooperation are of little comfort to those who confront the realities of loss of mission-critical data, carefully-crafted online reputations, and client confidentiality.

\(^\text{19}\) See FYI \textit{supra} note 4, at ¶ 16 (listing data retrieval as one of the items a potential cloud user should be concerned with).


\(^\text{21}\) Nicole Black, \textit{Technology: Lawyers should not be Wary of Cloud Computing}, 72 \textit{Tex. B.J.} 746, 746 (2009) (discussing the concerns attorneys may have when using cloud services).


5
I. How Cloud Computing Works

Cloud computing is “a platform for the delivery of software services and other applications through remote file servers. Rather than storing and accessing information on your desktop computer, your data and software exist on remote servers and are accessible wherever you happen to be.”23 Organizations can deploy a cloud in at least two ways: (1) as a private cloud—implemented within an organization using that organization’s infrastructure, or (2) as a public cloud—an advertiser-supported or fee-based service offered over the Internet.24 Though private clouds may create some of the same risks as public clouds, the public cloud most concerns policy-makers and industry leaders.25 The industry generally divides public clouds into three species: (1) Software-as-a-Service, (2) Platform-as-a-Service, and (3) Infrastructure-as-a-Service.26

A. Software-as-a-Service: Familiar Places on the Web

Software-as-a-Service (SaaS) is the simplest view of cloud computing and includes familiar services like Facebook, YouTube, webmail, e-commerce sites like Amazon.com, online gaming sites such as WorldofWarcraft.com, and even legal research sites like LexisNexis and Westlaw.27

---

25 See Smith Speech, supra note 23 (discussing public policy, security, and privacy concerns).
26 Pijanowski, supra note 11.
27 Smith Speech, supra note 23.
Usually, a SaaS vendor does business directly with an end-user. But SaaS is really just a repackaging of an older service-delivery model.

During the dot-com boom, many vendors used the Internet to deliver services under what was called an “application service provider” (ASP) model. Because broadband services were not yet widely available, ASP applications generally comprised very simple web pages or reports and allowed consumers to complete simple transactions like buying a book or a CD. But the widespread availability of broadband services to a large segment of the public breathed new life into web-based applications and increased the variety and capability of online application offerings.

Under the SaaS model, a user interacts with an online service through the Internet, and the online service’s vendor provides the necessary software applications and remote data storage. That storage may house the documents a user creates (such as a legal opinion letter or set of

---

28 Pijanowski, supra note 11. An end-user is someone who makes personal or business use of software. See id.
29 Kennedy, supra note 3.
32 Petro, supra note 30.
33 Pijanowski, supra note 11; Figure 1, infra.
accounting books), the user’s personal online identity (such as a seller rating or a “friends” list),
or the user’s financial information (such as credit card and checking account numbers).

Imagine once again that you want to set up that solo law practice or new business. Because of the availability of SaaS-based document management, e-mail, and accounting applications, it may now be possible for you to limit your in-house information technology (IT) needs to nothing more than cheap desktop computers, a simple peer-to-peer network, and a broadband Internet connection. Using SaaS generally allows you to pay for software and technical support on a monthly basis—which is considerably cheaper than investing in shrink-wrapped software and server hardware. It frees you from worrying about purchasing new releases or installing security updates. And it provides an easy way to expand your usage as your operation grows.

Some studies have shown a return-on-investment of almost 600% for a business that adopts SaaS.

But there are risks to using SaaS in your operation. To some extent, you give up control over your data because much of it is stored in some unknown location in the cloud. That could be a grave concern if you are handling confidential or time-sensitive information. And you

---
35 See Petro, supra note 30 (describing how a company outsourced all its back office applications to SaaS vendors).
36 FYI, supra note 4, at ¶¶ 7-8.
37 Id.
38 Id.
40 See, e.g., Kennedy, supra note 3; FYI, supra note 4, at ¶¶ 14-17.
41 Kennedy, supra note 3.
42 Id.
have little control over the security practices of the cloud vendor.\textsuperscript{43} Without a solid service-level agreement (and perhaps even with one), your operation could grind to a halt because your SaaS vendor goes down or, even worse, goes out of business.\textsuperscript{44} Any of these events could leave your business at a standstill and cause permanent damage from irrevocable data loss.\textsuperscript{45}

B. Platform-as-a-Service: Databases, Large-Scale Storage, and Web Servers

Other, more complex business ideas may require you to go a step beyond SaaS. If your aspirations involve the delivery of your own software applications to end-users across the web, Platform-as-a-Service (PaaS) offers a way to do that.\textsuperscript{46} Now imagine that you would like to create a new nonprofit lawyer-referral service.\textsuperscript{47} You will probably hire a programmer or two and perhaps some technical support and network administration staff. You will still need to purchase desktop computers, set up a network in your office, and make sure you have a broadband connection to the Internet just as you would if you were setting up a small law practice or business. But how will you make your new application available to customers on the web? You could jump in with both feet, buy some server hardware and software, and maintain your web and database servers yourself—an expensive and time-consuming proposition. Or you could take advantage of a PaaS offering from a vendor like Microsoft or Amazon.\textsuperscript{48}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{43} Id.
\item \textsuperscript{44} Id.
\item \textsuperscript{45} Id.
\item \textsuperscript{46} Id.
\item \textsuperscript{47} Pijanowski, supra note 11.
\item \textsuperscript{48} E.g., www.lawyers.com, Lawyer, Attorney, Law Firms, Attorneys, Legal Information. Lawyers.com (last visited Mar. 9, 2010).
\item \textsuperscript{49} See Pijanowski, supra note 11 (describing Platform-as-a-Service vendors and functions).
\end{itemize}
\end{footnotesize}
PaaS allows you to develop your application and deploy it on someone else’s servers in the cloud. Your users will have no idea that you are not hosting the web site yourself, and from their point of view, your new referral service appears to be just another SaaS application. Your programmers can develop and release the application using the PaaS vendor’s tools and cloud services. The vendor’s cloud services usually include web servers, storage capabilities, user authentication, backup, and billing, among other things. These services allow you to concentrate on developing and maintaining your software application rather than devoting precious resources to ancillary business and operational functions.

Another advantage of using PaaS to deploy an application is that you can scale resources according to your needs. As your business grows, you can easily add additional storage or web capacity simply by uploading a new configuration file to the cloud service or by changing settings in your cloud vendor’s control panel. As with SaaS applications, PaaS generally requires you to pay as you go. A vendor may charge by the amount of storage or computing power you use, or by the load your customer traffic creates.

But there is a price to pay for this convenience. You not only have the same kinds of security and data-control concerns a SaaS user has; delivering your application using PaaS adds a cloud

---

49 Figure 2, infra.
50 Id.
52 Pijanowski, supra note 11; Figure 2, infra.
53 Pijanowski, supra note 11.
54 Id.
55 Id.; see also Part I.A, supra.
56 Pijanowski, supra note 11.
provider to the contractual and technical mix. In some ways, you have doubled your exposure since either your own software application or the PaaS vendor’s failure could cause security and down-time issues. Because you are limited to the PaaS vendor’s development tools, you probably cannot take advantage of third-party software to supplement your application. And because the cloud vendor provides the run-time environment for your software—the operating system and services your software uses—you cannot easily change vendors. This puts you in a position of strong dependence on your cloud vendor, which could be devastating if the vendor decides to change its development tools, run-time environment, or simply goes out of business.

C. Infrastructure-as-a-Service: Large-Scale Application Deployment in the Cloud

There is yet another alternative that offers still more flexibility and capability. Assume that your lawyer-referral service has grown and that your users are clamoring for you to expand your services to compete directly with online research tools such as Westlaw and LexisNexis. That kind of development effort is far more demanding. Creating a successful product would require you to build a far more complex technology architecture that uses a greater variety of computing platforms. You would need large-scale data storage to house millions of documents, industrial-scale computing power to search those documents, and nimble web interfaces to deliver documents to your users.

---

58 Id.
59 Pijanowski, supra note 11; Reeves, supra note 57.
60 Pijanowski, supra note 11; Reeves, supra note 57.
61 See Part I.A, supra.
Again, you could opt to build a large data center containing a myriad of database, web, file, and application servers. But such an enterprise could cost millions and require a small army to set up and maintain. It would require you to worry about complex issues wholly unrelated to the main thrust of your business including wiring, electricity, fail-over services, backup power supplies, industrial-strength air conditioning, and fire-suppression systems. You would have to continually apply software updates and security patches and continuously monitor system performance. Simply procuring and maintaining the proper number and kind of server software licenses for your data center would be a full-time job. And you would be hard-pressed to estimate the amount of hardware and bandwidth you would need—an unforgiving and constantly moving target with a large price tag attached to inaccurate guesses.

Fortunately, there are companies out there that have already done many of these things for you and offer data-center services in the cloud under the aegis of Infrastructure-as-a-Service (IaaS). Unlike PaaS, IaaS does not limit your choice of development tools and run-time environments. Instead, you create a “virtual machine”—a set of specifications that defines your development and run-time environment as though you purchased and set up the hardware and software in your shop—and upload it to the cloud vendor. You can specify the operating

---

63 Id.
64 Id.
66 Id.
67 Id.
68 Pijanowski, supra note 11.
69 Id.
70 Id.; see also Figure 3, infra.
systems, database systems, and web servers your application uses.\textsuperscript{71} Like PaaS, IaaS allows you to scale the resources you use according to your needs.\textsuperscript{72} And you can still use the cloud provider’s ancillary services (such as user authentication, backup, and the like), but you are not required to.\textsuperscript{73} Also like PaaS, IaaS services are generally priced on a pay-as-you-go basis and depend on the amount of storage, bandwidth, and computing power you use.\textsuperscript{74}

But unlike the development and run-time lock-in problem PaaS presents, IaaS is more likely to allow you to change cloud vendors if and when you need to.\textsuperscript{75} Under the IaaS model, you take on more responsibility for choosing your development tools and runtime environment and for developing your software application.\textsuperscript{76} But the IaaS provider is still responsible for providing the server hardware, software, maintenance, related ancillary services, and your application’s presence on the web.\textsuperscript{77}

Still, there are additional risks that flow out of these additional capabilities. Those risks include the risks inherent in the SaaS and PaaS models.\textsuperscript{78} But the added complexity and control you gain from specifying your own configuration shifts many of those risks from the cloud service provider directly to your operation. Now that you are providing a more mission-critical function (a service on which your clients depend to maintain their business operations), your clients may want you to provide service-level agreements that require you to guarantee “performance, uptime, quality of service, incident management, escalation and penalties.”\textsuperscript{79} But

\begin{itemize}
\item \textsuperscript{71} Pijanowski, \textit{supra} note 11.
\item \textsuperscript{72} Id.
\item \textsuperscript{73} Id.
\item \textsuperscript{74} Id.; see also Part I.A, \textit{supra}.
\item \textsuperscript{75} Pijanowski, \textit{supra} note 11.
\item \textsuperscript{76} Id.
\item \textsuperscript{77} Pijanowski, \textit{supra} note 11.
\item \textsuperscript{78} See Part I.A, \textit{supra}.
\item \textsuperscript{79} Kennedy, \textit{supra} note 3.
\end{itemize}
the benefits of cloud computing likely outweigh the difficulties and risks because of the prospect of a significant return on investment and a dramatic reduction in hardware and software maintenance and management headaches.  

D. Advantages and Benefits of Cloud Computing

Cloud computing offers enormous potential benefits. Users can access applications and data from anywhere at any time they choose. And cloud applications can greatly enhance a user’s ability to cooperate and collaborate. Cloud providers decentralize data, creating greater redundancy and less vulnerability to natural and man-made disasters. They can employ highly-trained specialists to deal with security, maintenance, and system issues. Cloud computing offers rapid and intelligent resource adjustment as well as economies of scale. But there are still roadblocks that industry and government must overcome before cloud computing can realize its full potential.

II. Barriers to Confidence in the Cloud

Cloud computing offers many advantages to organizations large and small, but the advantages are not without risks. The complex web of relationships in cloud computing creates can compound the difficulty of contractual compliance. At the core of these issues are concerns over security, confidentiality, and ownership of electronic data as well as liability for system

---

80 See Part I.A, supra.
81 Smith Whitepaper, supra note 15, at 1; see also ENISA REPORT, supra note 12, at 17.
82 Smith Whitepaper, supra note 15, at 1.
84 ENISA REPORT, supra note 12, at 17.
85 Id. at 17-18.
86 Id. at 18-20.
breakdowns. More than two centuries ago, Thomas Jefferson wrote that “the infidelities of the post office and the circumstances of the times are against my writing fully and freely.” So worries about the security and reliability of information systems are nothing new. And concerns about liability for simply delivering a message are even older. Like the poor Amalekite that told King David of the deaths of Saul and Jonathan, cloud providers face the unwanted prospect of official entanglement or punishment for merely acting as an information conduit.

Jurisdictions around the world are grappling with issues of security and privacy. Some U.S. courts have held that cell-phone location-tracking information is protected by the Fourth Amendment. But the Obama administration disagrees. The British government is pushing ahead with a national DNA database that provides the government with a permanent source of information about its citizens’ most personal characteristics. But the German high court just struck down a law allowing authorities to “retain data on telephone calls and e-mails, saying it marked a ‘grave intrusion’ into personal privacy rights and must be revised.” Industry leaders and legislators have pushed for more reasonable limits on government access to electronic

87 See ENISA REPORT, supra note 12, at 7-8.
89 Second Samuel 1:1–15 (King James).
90 ENISA REPORT, supra note 12, at 5.
91 E.g., In re U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008).
communication. But the Obama administration seeks to expand warrantless surveillance of the Internet.

There are four distinct categories of concerns that create barriers to wider acceptance of cloud computing. First, there are issues the technology creates such as loss of governance and control, the failure of security and separation mechanisms, reliability, and malicious destruction of data. Second, ownership and control of online data is sometimes uncertain and can be abused or misused. Third, there are concerns over law enforcement’s access to confidential data under the Fourth Amendment. And fourth, the current law that governs most online communication is almost twenty-five years old and there is a sense that technology has passed it by.

A. Technological Barriers to Acceptance of Cloud Computing

Reliability is one of the main concerns of any computer user. For a cloud computing application to run successfully, many moving parts must operate well together, including the user’s desktop hardware and operating system, web browser, and Internet connection; the cloud provider’s Internet connection, hardware, and software; and the software vendor’s application and any third-party components the vendor’s application uses. The recent problem-filled history of Microsoft’s Vista operating system—which had troubles ranging from printing...

---

95 See In Re App. for Pen Regg & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (noting that in 2000, legislators introduced a bill to require a showing of probable cause to gain access to cell phone location information); Smith Whitepaper, supra note 15, at 3 (calling for greater Fourth Amendment protection).
97 ENISA REPORT, supra note 12, at 9-10; Murley, supra note 83, at 252-53.
98 Picker, supra note 20, at 7-9.
99 Smith Whitepaper, supra note 15, at 3.
100 Dempsey, supra note 14, at 67-70.
101 See Figure 1-3, infra.
documents to bogged-down performance—shows that this can be a challenge.\textsuperscript{102} Even the largest providers can experience outages—as with Google’s Gmail.\textsuperscript{103} And sometimes software vendors fail to deliver software that fulfills speed and reliability guarantees.\textsuperscript{104} Despite these considerable technical hurdles, internet use continues to rise and with it, the opportunities for new businesses based on cloud computing.\textsuperscript{105}

But aside from these concerns, attention to malicious breaches of privacy and security still drive much of the discussion about cloud computing.\textsuperscript{106} Traditional malicious hacking through viruses, worms, and similar means remains a danger, but the cloud computing paradigm creates new risks. Because a cloud provider might store data from many users—especially corporate users implementing a PaaS or IaaS structure—on the same physical hardware, there is a risk of isolation failure.\textsuperscript{107} That is, a provider could inadvertently or intentionally commingle data from multiple clients (a “guest-hopping” attack).\textsuperscript{108} There is also a risk that a provider’s employees (malicious insiders) could damage a client’s data or infrastructure.\textsuperscript{109} Cloud computing opens new points of entry for malicious attacks as well. Web-based management interfaces for configuring a client’s cloud resources combined with the traditional vulnerabilities of web

\textsuperscript{103} Kennedy, supra note 3. On September 1, 2009, Gmail experienced an outage that lasted roughly one-hundred minutes. Press Release from Ben Treynor, VP Engineering and Site Reliability Czar, Gmail, More on Today’s Gmail Issue (Sept. 1, 2009), http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html.
\textsuperscript{104} See Petro, supra note 30 (describing severe performance and reliability issues with an online legal practice management application).
\textsuperscript{105} Lee Rainie, \textit{Internet, Broadband, and Cell Phone Statistics} 10 (Jan. 5, 2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_December09_update.pdf
\textsuperscript{106} E.g., Smith Whitepaper, supra note 15, at 2-3; \textit{Open Cloud Manifesto}, supra note 15, at 3-4; \textit{ENISA REPORT}, supra note 12, at 8-10.
\textsuperscript{107} \textit{ENISA REPORT}, supra note 12, at 9.
\textsuperscript{108} \textit{Id}.
\textsuperscript{109} \textit{Id} at 10.
browsers also create new security holes. And the loss of direct control over hardware and software creates headaches for more sophisticated users.

Cloud computing may also lead to legal compliance issues regarding information security. Government agencies and contractors must make sure that their cloud service providers comply with certain security protocols such as those established by the National Bureau of Standards and the NSA under the Computer Security Act. Insecure or incomplete deletion of classified material could create a serious liability issue for both the cloud service provider and its clients. “Covered entities” under the Health Insurance Portability and Accountability Act (HIPAA) must comply with certain privacy and confidentiality procedures. A breach of these procedures can result in stiff penalties for an employer or even an employee. And public companies that fail to obtain SAS 70 qualification by adhering to certain procedures and controls can easily lose the confidence of investors and customers. It may be difficult to tell whether a provider’s security practices comply with these statutes, regulations, and standards. Such a lack of transparency creates a real obstacle to widespread adoption.

110 Id. at 9-10; Open Cloud Manifesto, supra note 15, at 4.
112 ENISA REPORT, supra note 12, at 10.
116 ENISA REPORT, supra note 12, at 9; Open Cloud Manifesto, supra note 15, at 3-4; Smith Whitepaper, supra note 15, at 6.
117 ENISA REPORT, supra note 12, at 9; Open Cloud Manifesto, supra note 15, at 3-4; Smith Whitepaper, supra note 15, at 6.
Other areas also lack transparency and standardization. Once users decide on a particular cloud provider, it could be very difficult for them to switch providers later because their information might be stored in a form that is unique to the original provider—the “lock-in” issue. The lack of standard data formats and application platforms “may lead to a catastrophic business failure should the cloud provider go bankrupt,” merge with another provider that has different standards, or fail for technical reasons. Though the risk of lock-in is great for PaaS and IaaS users, it is probably most acute for SaaS users. This is because PaaS and IaaS users are generally application developers who have the technical savvy needed to plan for the lock-in scenario. But the stakes are still very high for PaaS and IaaS users because they have obligations to their own client communities. And PaaS and IaaS users still face a significant impediment to providing a good customer experience because there are no standard metering and monitoring tools they can use to measure the cloud provider’s performance.

Finally, there are a number of other technical risks associated with cloud computing such as data interception or leakage. Most are generally not unique to cloud computing and will likely exist no matter what method a user undertakes to use or deploy a software application. But even if industry and government somehow overcome these technical hurdles, other significant concerns will continue to exist such as ownership and control of personal data.

---

118 ENISA REPORT, supra note 12, at 9; Open Cloud Manifesto, supra note 15, at 4.
119 ENISA REPORT, supra note 12, at 26.
120 See Figure 2-3, infra.
121 Id.
123 See ENISA REPORT, supra note 12, at 38-43, 47-52 (describing various risks associated with but not necessarily specific to cloud computing).
124 Id.
B. Ownership and Control Barriers to Acceptance of Cloud Computing

In 2008, the Pew Internet & American Life Project reported that 69% of all Internet users had “either stored data online or used a web-based software application.”125 Yet, the same study showed that a majority of users were very concerned with how cloud providers might use their personal data.126 And the Federal Trade Commission (FTC) expressed concern that large amounts of data collected by cloud providers might be employed in ways that users did not intend and do not understand.127

Professor Randal C. Picker has pointed out that cloud computing centralizes data flow and processing, creating a rich “clickstream” of information for the cloud provider.128 Clickstream data is information that is captured by a cloud provider as a user works and includes such things as buying patterns, search histories, and personal information.129 Professor Picker noted that cloud providers sometimes use the content of e-mails or other documents stored in the cloud provider’s system to create directed advertising—raising serious concerns of confidentiality and ownership of content stored in the cloud.130 Does the cloud provider’s physical possession of data create ownership rights in that data? Consumers might sometimes expect to see directed advertising based on their Internet habits, but other uses of that information may be troubling.131 For example, the Associated Press recently reported that the federal government used shopper-card data—data generated when a retailer swipes or scans a consumer’s retailer-specific discount

---

126 Id. at 7.
127 Smith Whitepaper, supra note 15, at n.1.
128 Picker, supra note 20, at 5-6.
129 Id.
130 Id. at 6.
131 Id.; Smith Whitepaper, supra note 15, at n.1.
card—to trace salmonella poisoning to its source.\footnote{David Mercer, \textit{CDC Uses Shopper-Card Data to Trace Salmonella}, \textit{ASSOCIATED PRESS} (Mar. 10, 2010), \textit{available at} http://news.yahoo.com/s/ap/20100311/ap_on_sc/us_shopper_card_sleuths.} Though, in that particular case, the Centers for Disease Control got permission from patients to use the data, some consumer-privacy advocates are concerned that the government may not ask for permission next time.\footnote{\textit{Id.}.} Professor Picker also pointed out a related problem—that of data “stickiness”—in the cloud.\footnote{Picker, \textit{supra} note 20, at 6-8.} Data stickiness is the build-up of information directly associated with a particular person.\footnote{\textit{Id.} at 6.}

Some social networking or transactional cloud applications allow users to create online identities or reputations. One such site, eBay, allows a user to “build up a reputation score transaction by transaction” to mitigate problems associated with transactions conducted “at a distance between strangers.”\footnote{\textit{Id.}.} ReverseAuction.com gleaned user IDs, e-mail addresses, and seller ratings from eBay’s web site and sent eBay users invitations offering to allow them to use their eBay identities on its site.\footnote{\textit{Id.} at 6-7.} As ReverseAuction found out the hard way, eBay’s user agreement required users not to import or export their reputation scores.\footnote{\textit{Id.}; Press Release, Federal Trade Commission, Online Auction Site Settles FTC Privacy Charges (Jan. 6, 2000), \textit{available at} http://www.ftc.gov/opa/2000/01/reverse4.shtm.} The issue of virtual property ownership is especially acute in the online-gaming industry and its resolution is a work in progress.\footnote{See generally Alisa B. Steinberg, \textit{For Sale—One Level 5 Barbarian for 94,800 Won: The International Effects of Virtual Property and the Legality of its Ownership}, \textit{37 GA. J. INT’L & COMP. L.} 381 (2009).} “Virtual property is property that gamers acquire in an online game” that may have “real-world value.”\footnote{\textit{Id.} at 382-83.}
Just as troubling than the issue of data ownership is the ability of a cloud provider to unilaterally change its user agreement to affect how consumers use their own computer hardware and software. Blizzard’s end-user license agreement (EULA) prohibits the use of “automation software (bots) . . . or any other unauthorized third-party software” that allow a user’s computer to play Blizzard’s online game when the user is not physically present. In 2009, a federal district court found a developer of that kind of “bot” liable for tortious interference with Blizzard’s user agreement. The defendant in that case is currently appealing the tortious interference claim before the Ninth Circuit. The outcome could have far-reaching effects on what types of end-user activities a service provider can limit through EULAs.

Farming out data-center services to a cloud provider necessarily means that a user will lose some measure of control over operations. Terms-of-use agreements may prohibit technical procedures a user would like to perform in order to test system vulnerability or system performance. And service-level agreements may not require the cloud provider to undertake that testing. That could create security gaps and compliance issues for the user. Further, the tangle of contractual agreements involving a cloud provider and its subcontractors, a cloud user, and the cloud user’s clients could further complicate operations to the point that complete

141 www.worldofwarcraft.com, World Of Warcraft End User License Agreement, http://www.worldofwarcraft.com/legal/eula.html. Blizzard is the company that provides the online multi-player game called World of Warcraft. Id.
144 ENISA REPORT, supra note 12, at 9.
145 Id. at 29.
146 Id.
147 Id.; Kennedy, supra note 3.
contractual compliance is impossible.\textsuperscript{148} And that tangle might also make it impossible to
manage and monitor license agreements a cloud user makes with its clients.\textsuperscript{149}

There is the risk that cloud users may completely lose control over their data or their client’s
data if they decide to switch providers, the provider fails for some reason, or the provider is
acquired by another firm.\textsuperscript{150} That could create severe liability issues for cloud users because of
their contractual responsibilities or because of the damage caused to their clients by a loss of data
or system access.\textsuperscript{151} These kinds of risks also create ethical dilemmas for those in the legal
profession because of their obligation to keep client information confidential.\textsuperscript{152}

Uncertainty over the security and confidentiality of data in the cloud should give lawyers
pause when considering whether to adopt SaaS applications in their practices.\textsuperscript{153} Fortunately, a
number of state bars have weighed in with favorable opinions on the responsible use of cloud
computing technology in law practices.\textsuperscript{154} The American Bar Association (ABA) issued an
opinion approving of a lawyer’s use of unencrypted e-mail to transmit information to a client
relating to the representation of the client.\textsuperscript{155} A New York bar opinion goes as far as allowing a
lawyer to use an e-mail service that scans e-mail content in order to generate advertising—as
long as human beings other than the sender and recipient cannot view the content.\textsuperscript{156} And while

\textsuperscript{148} Id. at 29-30; see also Open Cloud Manifesto, supra note 15, at 4.
\textsuperscript{149} ENISA REPORT, supra note 12, at 47.
\textsuperscript{150} ENISA REPORT, supra note 12, at 9; Open Cloud Manifesto, supra note 15, at 4.
\textsuperscript{151} ENISA REPORT, supra note 12, at 31.
\textsuperscript{152} See FYI, supra note 4, at ¶¶ 14-16.
\textsuperscript{153} Id. at ¶ 14; Kennedy, supra note 3; but see Black, supra note 21, at 747 (encouraging
responsible use of cloud computing technology).
\textsuperscript{154} NEW YORK STATE BAR ASS’N, COMM. ON PROF’L ETHICS, OP. 820 (2008); N.J. SUPREME
COURT ADVISORY COMM. ON PROF’L ETHICS, OP. 701 (2006); NEV. STATE BAR STANDING
COMM. ON ETHICS & PROF’L RESP., FORMAL OP. 33 (2006); ABA, STANDING COMMITTEE ON
ETHICS AND PROFESSIONAL RESPONSIBILITY, FORMAL OP. 99-413 (1999).
\textsuperscript{155} OP. 99-413.
\textsuperscript{156} OP. 820.
New Jersey and Nevada ethics opinions allow lawyers to store client documents electronically in storage that they may access remotely, they require that a lawyer use reasonable care and act competently to ensure the confidentiality of the data.\textsuperscript{157} Maine and Florida have similar requirements.\textsuperscript{158} Though these ethics opinions are a step in the right direction, uncertainty remains. And there are other legal issues—including constitutional and statutory problems—that pose risks to users and providers of cloud services.

C. The Fourth Amendment and the Government’s Access to Data in the Cloud

Upon a cursory glance, the Supreme Court’s Fourth Amendment doctrine would seem to support strong protection against government searches and seizures of data in the cloud. That might comfort the 64% of respondents to a recent survey who said they would be concerned if cloud providers handed their data over to law enforcement when merely asked to do so.\textsuperscript{159} But the uneven application of Fourth Amendment principles to Internet technology still poses risks to cloud users.

The Fourth Amendment dictates that people have a right to protection against “unreasonable searches and seizures.”\textsuperscript{160} The threshold question in any Fourth Amendment case is whether a search has occurred.\textsuperscript{161} The Supreme Court held, in \textit{Katz v. United States},\textsuperscript{162} that “the Fourth Amendment protects people, not places.”\textsuperscript{163} In his concurrence, Justice Harlan said that a search without a warrant is presumptively unreasonable if it occurs in an area where a person has a

\textsuperscript{157} Op. 701; Op. 33.
\textsuperscript{159} Horrigan Memo, \textit{supra} note 125, at 7.
\textsuperscript{160} U.S. CONST. amend IV.
\textsuperscript{161} 389 U.S. 347 (1967).
\textsuperscript{162} \textit{Id.} at 353.
\textsuperscript{163} \textit{Id.} at 351.
“reasonable expectation of privacy.”

Justice Harlan went on to point out that the state may violate that reasonable expectation of privacy by electronic as well as physical means—by a wiretap as well as a physical trespass.

The Supreme Court later adopted Justice Harlan’s test as the “touchstone of Fourth Amendment analysis.” The Court established a two-part inquiry for whether a person has a “constitutionally protected reasonable expectation of privacy.” First, did the person manifest “a subjective expectation of privacy in the object of the challenged search?” That is, did the person show “that he sought to preserve something as private?” And second, “is society willing to recognize that expectation as reasonable?” More recently, the Court held that a prohibited search occurs when law enforcement uses surveillance technology that the general public does not use. And the Court has reinforced its position that the government may not search letters, sealed packages, and closed containers without a search warrant.

These restrictions on government intrusion might look encouraging to users and providers of cloud computing because it seems logical to analogize data on a secured server to a sealed package or closed container. And computer forensics requires a person to have skills and tools

---

164 Id. at 360-61 (Harlan, J., concurring).
165 Id. at 362 (Harlan, J., concurring) (emphasis in original).
167 Id.
168 Id.
170 Ciraolo, 476 U.S. at 211.
the general public does not use. But the Supreme Court’s jurisprudence has taken other turns that erode any sense of security. In *Smith v. Maryland*, the Court held that the Fourth Amendment protects the content of a phone conversation, but it does not protect the numbers a person dials. And long ago, the Court held that the Fourth Amendment protects the content of letters and packages deposited in the U.S. Mail, but not their exteriors. The obvious conclusion is that this principle could apply to web addresses, e-mail addresses, and subscriber information—and the lower courts have not disappointed in that regard. For example, the Ninth Circuit held that the government could install a surveillance device at an Internet Service Provider’s (ISP) facility to capture web address information. And the Tenth Circuit held that “subscriber information provided to an Internet provider is not protected by the Fourth Amendment’s privacy expectation.”

These holdings are also in keeping with the Supreme Court’s Fourth Amendment third-party doctrine. The third-party doctrine made a significant appearance in *United States v. Hoffa*. The Supreme Court held that the Fourth Amendment did not apply to statements Jimmy Hoffa made to a paid government informer. Then, in *Couch v. United States*, the Court held that there could be no reasonable expectation of privacy for records handed over to an accountant-

---

175 442 U.S. 735 (1979).
176 *Id.* at 744-45.
177 Ex parte Jackson, 96 U.S. 727, 733 (1877).
178 United States v. Forrester, 495 F.3d 1041, 1049 (9th Cir. 2007); United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008);
179 *Forrester*, 495 F.3d at 1049.
180 *Perrine*, 518 F.3d at 1204-05.
182 *Id.*
Extending the doctrine a bit further, the Court held that a bank depositor had no Fourth Amendment protection over bank records held by the depositor’s bank. Because this line of cases denies protection to people who give information to professional service providers, they do not bode well for users who store private or confidential data in the cloud with third-party vendors.

The lower courts have struggled to make sense of the Supreme Court’s Fourth Amendment doctrine when applying it to electronic communication and internet technology. One district court held that though a web site is like a “file cabinet or other physical container[],” users that store information on a web site assume the risk that a third party may reveal that information to authorities. The court held that even though the web site was password-protected, and even though the defendants may have had a subjective expectation of privacy, storing data on a web site is not something society would regard as reasonably private.

But the Fourth Circuit held that a different kind of third party—a live-in girlfriend—could not consent to a police search of her boyfriend’s files on their shared computer. In what is a more rational approach to the closed container principle, the court found that the Fourth Amendment protected the boyfriend’s files because they were password-protected and inaccessible to the girlfriend. Yet the Tenth Circuit held that a father could consent to a police search of his adult son’s password-protected computer.

---

184 Id. at 335.
187 Id. at 120, 123 (citing Smith v. Maryland, 442 U.S. 735, 744-45 (1979)).
188 Trulock v. Freeh, 275 F.3d 391, 398, 403 (4th Cir. 2001).
189 Id.
190 United States v. Andrus, 483 F.3d 711, 719-22 (10th Cir. 2007).
In an institutional application of Fourth Amendment third-party doctrine, the Tenth Circuit held that a university professor had no reasonable expectation of privacy because he should have known that network administrators could view the content on his university-owned computer.\textsuperscript{191} But a district court in the Seventh Circuit held that a state employee \textit{did} have a reasonable expectation of privacy in her government-issued laptop because the employee had no notice that it was subject to search.\textsuperscript{192} The Ninth Circuit Court of Appeals seemed to return to the closed-container principle.\textsuperscript{193} It held that police officers had a reasonable expectation of privacy concerning text messages sent on department-issued pagers.\textsuperscript{194} But it analogized e-mails to letters and held that while the content of electronic communication was protected under the Fourth Amendment, the identities of the sender and recipient were not.\textsuperscript{195} The Second Circuit has been a bit less equivocal, holding that an owner of a private computer in a private office has a reasonable expectation of privacy.\textsuperscript{196} But once law enforcement establishes that it is entitled to search a computer, how far does the scope of that search extend?

In what is probably a disturbing development for advocates of cloud computing, the circuits are split on whether a search for one purpose allows the government to dragnet unrelated information from a computer.\textsuperscript{197} Known as the “plain-view exception,” the Supreme Court has held that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”\textsuperscript{198} The Ninth Circuit held that police \textit{could} use

\begin{itemize}
\item \textsuperscript{191} United States v. Angeyine, 281 F.3d 1130, 1134-35 (10th Cir. 2002).
\item \textsuperscript{192} Maes v. Folberg, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007).
\item \textsuperscript{193} Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905-06 (9th Cir. 2008).
\item \textsuperscript{194} \textit{Id.}
\item \textsuperscript{195} \textit{Id.}
\item \textsuperscript{196} Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001).
\item \textsuperscript{197} \textit{Compare} United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003), \textit{with} United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).
\item \textsuperscript{198} Katz v. United States, 389 U.S. 347, 351 (1967).
\end{itemize}
evidence of child pornography taken from a defendant’s computer even though the search warrant was for evidence of a homicide.\textsuperscript{199} But the Tenth Circuit ruled that police could \textit{not} use child pornography evidence taken from a suspect’s computer when the search warrant was for evidence of the sale of narcotics.\textsuperscript{200} And the Ninth Circuit seemed to reverse course when it laid out stringent procedures the government must follow to segregate untargeted computer data and prohibited retention or examination of that untargeted data.\textsuperscript{201} This confusion among the circuits should trouble cloud computing users because cloud providers often store multiple users’ data on the same physical medium.\textsuperscript{202} So not only do users run the risk of the cloud provider’s isolation failure, they may also run the risk of law enforcement’s isolation failure in conducting a search unrelated to their data.\textsuperscript{203}

The courts have increased this danger of isolation failure by allowing broad search and seizure authority over computer hardware and physical media as well—not just data.\textsuperscript{204} In \textit{Upham}, the First Circuit upheld the validity of a warrant that authorized seizure of “any and all computer software and hardware, . . . computer disks, [and] disk drives” to allow the police to search for child pornography images off site.\textsuperscript{205} The implication of this ruling for innocent cloud users is staggering. If police seize hardware from a provider to look for information belonging to a particular user, that seizure could adversely affect otherwise uninvolved, innocent users. Though the Ninth Circuit also allows this kind of blanket seizure, it requires law enforcement to

\textsuperscript{199} \textit{Wong}, 334 F.3d at 838.
\textsuperscript{200} \textit{Carey}, 172 F.3d at 1273.
\textsuperscript{201} United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1000-01 (9th Cir. 2009).
\textsuperscript{202} ENISA REPORT, \textit{supra} note 12, at 9.
\textsuperscript{204} United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).
\textsuperscript{205} \textit{Id.} at 535, 537.
explain why an on-site search is not feasible.\textsuperscript{206} And even the recent \textit{Comprehensive Drug Testing} decision from the Ninth Circuit fails to take shared resources in the cloud into account and treats searches of electronic data as though they occur in isolation on a single computer.\textsuperscript{207} Technology has overtaken Fourth Amendment jurisprudence and Congress has done little with statutory law to make up for it.

\textbf{D. Inadequate Statutory Law: The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act}

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA).\textsuperscript{208} In 1994 and 1996, Congress amended the ECPA to place a higher standard on law enforcement’s access to electronic data and heighten privacy protection.\textsuperscript{209} The ECPA prohibits interception or disclosure of “any wire, oral, or electronic communication” except under certain conditions.\textsuperscript{210} It also prohibits law enforcement from using any illegally intercepted communication.\textsuperscript{211} And it requires law enforcement to follow detailed procedures to gain authorization to intercept electronic communications.\textsuperscript{212} It not only provides criminal penalties for violations, but it also

\begin{footnotesize}
\begin{enumerate}
  \item United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006).
  \item See \textit{Comprehensive Drug Testing}, 579 F.3d at 1000-01.
  \item Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C §§ 2510-22, 2701-12, 3121-27). The Act contains three main sections: Title I, §§ 2510-22, protects wire, oral, and electronic communications while in transit and amends Title III of the Omnibus Crime Control and Safe Street Act, commonly known as the Wiretap Act; Title II, §§ 2701-12, contains the Stored Communications Act (SCA), which protects communications held in electronic storage; and Title III, §§ 3121-27, the Pen Register Act, restricts the use of pen registers—devices that record dialed telephone numbers.
  \item § 2511(1)(a), (c).
  \item § 2515.
  \item §§ 2516-19.
\end{enumerate}
\end{footnotesize}
creates a private right of action against violators.\textsuperscript{213} The Second Circuit has held that even the government is subject to civil liability under the ECPA.\textsuperscript{214} But one of the main problems with the ECPA is that the definition of “intercept” is vague and relies on an outdated understanding of “communication.”\textsuperscript{215} An intercept is “the aural or other acquisition of the contents of any wire, electronic, or oral \textit{communication} through the use of any electronic, mechanical, or other device”—which could (and should) apply to any data in the cloud.\textsuperscript{216}

What constituted a “communication” in 1986 when Congress passed the ECPA may have been obvious to those familiar with the technology of the time, but as technology has changed, courts have struggled to clarify its meaning. In \textit{United States v. Councilman},\textsuperscript{217} the First Circuit ruled that copying e-mails from transient storage was a prohibited interception under the ECPA.\textsuperscript{218} But the dissent in that case pointed out that many other circuit and district courts had held just the opposite.\textsuperscript{219} In \textit{United States v. Scarfo},\textsuperscript{220} the district court held that the government’s use of a keystroke logger (a device that captures keystrokes as they are entered) did not violate the ECPA.\textsuperscript{221} The court reasoned that because the government did not use the

\textsuperscript{213} §§ 2511(4), 2520.
\textsuperscript{214} Organizacion J.D., Ltda. v. DOJ, 18 F.3d 91, 94-95 (2d Cir. 1994) (per curiam).
\textsuperscript{216} Id. (emphasis added).
\textsuperscript{217} 418 F.3d 67 (1st Cir. 2005) (en banc).
\textsuperscript{218} Id. at 79.
\textsuperscript{220} 180 F. Supp. 2d 572 (D.N.J. 2001).
\textsuperscript{221} Id. at 581.
keystroke logger “during any period of time in which the computer’s modem was activated,” and therefore the defendant’s computer was not connected to any outside service, capturing keystrokes did not affect any electronic communication.\textsuperscript{222} That ruling presupposed a technological world in which users have to consciously activate an Internet connection and generally stay connected for only short periods. Such a supposition is surely obsolete in today’s world of broadband Internet connections that are always on, always connected.\textsuperscript{223} And confusion over interception has a ripple effect that disrupts other parts of the ECPA.

The Stored Communication Act (SCA), Title II of the ECPA, governs information held in electronic storage.\textsuperscript{224} The SCA prohibits intentional access, without or exceeding authorization, to electronic communications stored in an electronic communication service if that access alters or prevents authorized access.\textsuperscript{225} It also prohibits providers of “electronic communication services” or “remote computing services” from improperly disclosing any electronic communication without consent—even to the government.\textsuperscript{226} There are exceptions to disclosure for search warrants, grand jury subpoenas, and court orders.\textsuperscript{227} And the service provider may access communications for its own purposes.\textsuperscript{228} The SCA creates a private right of action, which also applies to government entities.\textsuperscript{229} For cloud providers, the definitions of “electronic

\textsuperscript{222} Id.
\textsuperscript{223} See Rainie, supra note 105, at 1 (noting that 60% of survey respondents in 2009 used broadband in their homes). Unlike today, Internet connections in the past were predominantly dial-up connections that required a user to connect to the Internet temporarily through a phone line. The Center for Education and Research in Information Assurance and Security, Broadband vs. Dialup Internet Connection, http://www.cerias.purdue.edu/education/k-12/cerias_resources/files/infosec_newsletters/06broadband.php (last visited Apr. 10, 2010).  
\textsuperscript{225} § 2701(a).  
\textsuperscript{226} § 2702.  
\textsuperscript{227} § 2707(e).  
\textsuperscript{228} § 2701(c)(1).  
\textsuperscript{229} § 2707(a); Organizacion J.D., Ltda. v. DOJ, 18 F.3d 91, 94-95 (2d Cir. 1994) (per curiam).
communication service” (ECS) and “remote computing service” (RCS) could be critical, but those definitions are unclear and outmoded. An “‘electronic communication service’ means any service which provides to users thereof the ability to send or receive wire or electronic communications.” A “‘remote computing service’ means the provision to the public of computer storage or processing services by means of an electronic communications system.” Both definitions apply equally well to just about every cloud computing service currently available, which could only lead to confusion in applying the SCA.

The SCA requires law enforcement to get a warrant to search messages stored in an ECS for 180 days or less. But if the message is stored for longer, then law enforcement can gain access to it under the far less onerous procedures that apply to a RCS. The procedures that relate to an RCS allow law enforcement access to stored communications by merely obtaining an administrative subpoena, grand jury subpoena, or court order—no warrant is required. Another distinction between the two types of services is that an ECS may voluntarily release a communication to law enforcement with the consent of the recipient while an RCS may release information with only the consent of the subscriber. Courts have struggled with these distinctions and their conclusions have been less than satisfying.

In Quon v. Arch Wireless Operating Company, the court concluded that an electronic-pager service was an ECS even though it stored messages in an archive and provided remote

---

231 § 2510(15).
232 § 2711(2).
233 § 2703(a).
234 § 2703(b).
235 Id.
236 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008).
237 Id.
messaging services.\textsuperscript{238} 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.\textsuperscript{239} The court tried to distinguish between storage and communication services, but under the cloud computing model, those types of services are utterly indistinguishable.\textsuperscript{240}

A faint glimmer of hope arose when the Sixth Circuit ruled that the SCA’s provisions and procedures allowing law enforcement to gain access to e-mails stored for more than 180 days were unconstitutional.\textsuperscript{241} A panel of that court ruled that even though the appellant’s service provider could scan the appellant’s e-mails for viruses, the appellant maintained a reasonable expectation of privacy in them.\textsuperscript{242} Unfortunately, the court later vacated its decision \textit{en banc} because it decided the issue was not yet ripe.\textsuperscript{243} But by treating all content the same regardless of whether it exists within an ECS or RCS, that decision directed the way to reform that is necessary to remove some of the barriers to wider acceptance of cloud computing.

In the same year that Congress passed the ECPA, the Computer Fraud and Abuse Act of 1986 (CFAA) became law.\textsuperscript{244} The CFAA makes it a crime to (1) access files without authorization and later transmit classified government information that “could be used” to injure the United States; (2) get information without authorization from financial institutions or private computers used in interstate commerce; (3) intentionally access a U.S. department or agency computer without authorization; (4) knowingly access a protected computer without authorization and with

\textsuperscript{238} Id. at 902.
\textsuperscript{239} See id. at 901 (quoting S. REP. NO. 99-541, at 2-3 (1986)).
\textsuperscript{240} Id.; see also Figures 1-2, infra.
\textsuperscript{241} Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), vacated \textit{en banc}, 532 F.3d 521 (6th Cir. 2008).
\textsuperscript{242} Id.
\textsuperscript{243} Id.
intent to defraud and get something of value; (5) knowingly transmit a program that intentionally causes damage to a protected computer, or intentionally access a protected computer and cause damage; (6) knowingly traffic in passwords of protected computers with intent to defraud; or (7) transmit, in interstate commerce, a threat to damage a protected computer with the intent to extort something of value.\textsuperscript{245} An attempt to violate any of these provisions is also a crime.\textsuperscript{246}

The CFAA seems to create a powerful deterrent to most computer crime, but some of its provisions lack the bite necessary to give many would-be criminals pause.\textsuperscript{247} The First Circuit ruled that a violation involving unauthorized access requires more than simply viewing information.\textsuperscript{248} A defendant must obtain something of value for a court to reach a conviction.\textsuperscript{249} Section 1030(a)(5) requires actual damage as a result of planting a virus or similar activity.\textsuperscript{250} Many times, actual damage may be difficult to ascertain or quantify.\textsuperscript{251} In the case of logic bombs—computer programs that lie in wait on a user’s computer and cause damage on a specific date or upon the occurrence of a specific event—the damage may not occur until much later.\textsuperscript{252} And the Act requires that to trigger felony penalties, any damage caused must exceed $5,000 in a one-year period.\textsuperscript{253} Because of the difficulty in determining the dollar amount of any damage, the CFAA seems to be yet another provision that lags behind the technological times and needs review and revision.

\begin{itemize}
\item \textsuperscript{245}§ 1030(a).
\item \textsuperscript{246}§ 1030(b).
\item \textsuperscript{247}See Smith Whitepaper, supra note 15, at 4-5 (describing additional tools law enforcement needs to combat malicious actors).
\item \textsuperscript{248}United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).
\item \textsuperscript{249}Id.
\item \textsuperscript{250}§ 1030(a)(5).
\item \textsuperscript{251}Smith Whitepaper, supra note 15, at 5.
\item \textsuperscript{252}See Kleindienst, supra note 13, at 318 (describing the delayed action of logic bombs).
\end{itemize}
III. Proposals to Enhance Confidence in the Cloud

In the recent past, a number of industry, nonprofit, and government-sponsored groups have publicized proposals to spur adoption of, and innovation and confidence in, cloud computing and the Internet. Some of these ideas include legislative proposals. Others include new industry standards. And still others embody elements of both.

A. Microsoft and the Cloud Computing Advancement Act

On January 20, 2010, Microsoft, through its Senior Vice President and General Counsel Brad Smith, announced a legislative and industry initiative it called the Cloud Computing Advancement Act. The proposal contains two main legislative thrusts: (1) modification of the ECPA to strengthen privacy protection, and (2) enhancement to the CFAA to deter malicious hacking. For industry, it proposes “truth in cloud computing principles” to allow users to assess whether a provider maintains adequate infrastructure and security controls. And finally, it proposes shoring up international jurisdictional questions through multilateral or bilateral cooperation. In the current environment, “[m]ultiple jurisdictions may have an interest in a single matter, each seeking access to user information.” And a lawful demand for information in one jurisdiction might lead to a prohibited disclosure in another.

254 See generally Smith Whitepaper, supra note 15; SCHWARTZ, supra note 17; Open Cloud Manifesto, supra note 15; ENISA REPORT, supra note 12.
255 See generally Smith Whitepaper, supra note 15; SCHWARTZ, supra note 17.
256 See generally Open Cloud Manifesto, supra note 15.
257 See generally ENISA REPORT, supra note 12.
259 Id. at 2-6.
260 Id. at 6-7.
261 Id. at 7-8.
262 Id. at 7.
263 Id.
While the proposal concedes that the courts must ultimately decide Fourth Amendment issues, it advocates that Congress update the ECPA by unifying the definitions “electronic communication service” and “remote computing service” to match a technological world in which there is no real distinction between them.\(^{264}\) This would eliminate confusion over which provisions of the ECPA apply to a given service.\(^{265}\) Further, the proposal asks for elimination of the distinction between e-mails stored for 180 days or less and e-mails stored for more than 180 days.\(^{266}\) And it supports previous calls for an omnibus federal privacy law to give users more “control over the data collected about them both online and offline.”\(^{267}\)

To deter malicious hacking, the proposal urges Congress to establish a presumed loss under the CFAA with a minimum multiplier of $500 for each unauthorized account a criminal accesses, making it easier to reach the statutory threshold of $5,000 that triggers felony penalties.\(^{268}\) And it asks Congress to impose a fine of $250,000 for each account the criminal accesses.\(^{269}\) It pushes for Congress to extend the private right of action under the CFAA beyond just the users a violation directly affects so that cloud providers can also sue violators.\(^{270}\) Finally, it calls for additional enforcement resources, including development of new forensic techniques.\(^{271}\)

\(^{264}\) Smith Whitepaper, \textit{supra} note 15, at 4.
\(^{265}\) \textit{Id.}
\(^{266}\) \textit{Id.; see also} Part II.D, \textit{supra}.
\(^{267}\) Smith Whitepaper, \textit{supra} note 15, at 4.
\(^{268}\) \textit{Id.}
\(^{269}\) \textit{Id.}
\(^{270}\) \textit{Id.}
\(^{271}\) \textit{Id.} at 6.
B. The Center for Democracy & Technology and Digital Search & Seizure

The Center for Democracy & Technology (CDT) also proposes enhancements to the ECPA.\(^{272}\) Specifically, it calls for Congress and the judiciary to require a showing of probable cause before allowing a seizure of online information without notice.\(^{273}\) But the CDT goes further in urging that Congress require a meaningful opportunity to object to subpoenas for online content in both civil and criminal cases.\(^{274}\)

C. IBM and the Open Cloud Manifesto

Like the Microsoft proposal, the *Open Cloud Manifesto* urges greater transparency in cloud computing operations to create consistency in operational controls among cloud providers.\(^{275}\) IBM and dozens of partners released the *Manifesto* to “initiate a conversation that will bring together the emerging cloud community.”\(^{276}\) It calls for cooperation between providers to establish standards for security, portability, interoperability, governance and management, and metering and monitoring.\(^{277}\) Such standards would minimize the lock-in issue and prevent providers from using their market strength to hold users hostage.\(^{278}\)

But the *Manifesto* cautions that standards must encourage innovation rather than stifle it.\(^{279}\) It points out that disparate, proprietary systems and programming models choke off the availability of skilled professionals—relegating many technical people to isolated niches.\(^{280}\) Like any other

---

\(^{272}\) SCHWARTZ, *supra* note 17, at 40.
\(^{273}\) *Id.*
\(^{274}\) *Id.*
\(^{275}\) *Open Cloud Manifesto, supra* note 15, at 4.
\(^{276}\) *Id.* at 1.
\(^{277}\) *Id.* at 6.
\(^{278}\) *Id.*
\(^{279}\) *Id.*
\(^{280}\) *Id.*
heady aspiration, the *Manifesto* will be only as good as its adherents. Unfortunately, two of the industry’s largest players, Microsoft and Amazon, have not signed on as supporters because they regard it as too vague and believe that it does not reflect their interests.\(^{281}\)

D. The European Union and the ENISA Report

Besides detailing a long list of security risks, the European Network and Information Security Agency (ENISA) recommends a set of procedures users can follow to protect themselves.\(^{282}\) The most important of these procedures is a recommended list of questions users should ask cloud providers.\(^{283}\) These questions include 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) legal requirements (location of data, governing jurisdiction, data recovery upon termination, subcontracts, and the like).\(^{284}\)

E. Beyond the Current Proposals: A Common-Sense Approach to Privacy, Security, and Ownership in the Cloud

The government must, as a practical matter, relegate many issues regarding cloud computing to private contracts between providers and users. Service-level agreements, metering and monitoring, fail-over, and backup are just a few of these issues.\(^{285}\) Industry proposals for

---


\(^{282}\) ENISA REPORT, *supra* note 12, at 71-90.

\(^{283}\) ENISA REPORT, *supra* note 12, at 71-83.

\(^{284}\) *Id.*

\(^{285}\) ENISA REPORT, *supra* note 12, at 66-68.
dialogue, standards, and new legislation are a good start, but the government can and should step in to alleviate other problems not addressed in those proposals. Because electronic communication inherently crosses jurisdictional boundaries, Congress should establish a comprehensive national framework that preempts state law to eliminate confusion and conflict between jurisdictions. The principle underlying that framework should be based on the idea that a user is entitled to ownership of data that is identified with the user whether the user created that data directly or indirectly through online activity. The framework should address three main areas of concern.

First, Congress should act to establish clear property boundaries in the ownership of data created and stored in the cloud and a bright-line boundary between remote online activities and desktop activities. A user’s carefully-crafted online reputation, such as a positive seller rating on eBay, should belong to the user—not to the forum where that reputation was, at least in part, established. A user’s interest in a positive seller rating is far stronger than the forum’s proprietary interest in it. How would the average person react if forced to sign a document at a car dealership stating that the dealership would not report the person’s positive payment history, but would allow the use of that history only to purchase cars at that particular dealership? It might be argued that a credit rating is built on more than a set of transactions with a single dealer whereas a seller rating applies only to a particular forum. But if every forum restricts a user’s control over personal information, then it would be impossible for users to cultivate and protect a comprehensive online reputation.

Congress should curtail the ability of online vendors to regulate the general activities on a particular user’s computer. What a user does with the software on their computer should be of

---

286 Smith Whitepaper, supra note 15, at 6-7.
no concern to the software vendor as long as it does not interfere with the vendor’s operations. The ability to craft useful extensions to established software applications attracts independent developers, increases innovation, and boosts user productivity. But overreaching EULAs can prohibit a user from employing third-party productivity software, stifling that innovation and productivity.

If the courts uphold EULAs that prohibit the use of “bots” on a user’s computer, then a predatory software vendor could wipe out productivity gains created by innovative third-party software simply by posting a new EULA to its web site that prohibits the use of third-party software with its products. How would people react if they were required to sign a document at a car dealership prohibiting the use of third-party cup holders in their new cars? How would they react to a letter from the car company telling them to remove all third-party cup holders from their cars? Certainly, people would be outraged if a dealership itself removed third-party cup holders from their cars during servicing. The electronic version of these scenarios could become reality if the Ninth Circuit upholds Blizzard’s tortious interference claim against MDY.

New legislation should prohibit software vendors from using “clickstream” data externally without a user’s permission because of the risk that the data may be used in ways the user does

---

289 Id.
not understand or approve of.\textsuperscript{291} Some vendors already ask for permission.\textsuperscript{292} Certainly, there are advantages to receiving advertising based on buying habits. But Congress should act to make such a use one of user preference. It should also prohibit selling or trading in that data without a user’s permission and allow users to manage the clickstream data their activities create. That would be in keeping with the spirit of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), which attempted to reduce the amount of unsolicited e-mail sent from a concealed or unknown source.\textsuperscript{293} Vendors who collect clickstream data should provide a mechanism that their users can employ to see the data and perhaps even delete it.

Second, Congress should amend the ECPA to require the government to overcome a very high threshold before it can seize hardware from a cloud provider that contains more than one user’s data.\textsuperscript{294} A single such seizure could disrupt the business transactions of thousands of businesses and perhaps even millions of users. In addition to heeding Microsoft’s recommendation to update the definition of the types of service providers, Congress should review and amend the ECPA with a definition of “interception” of electronic data that explicitly encompasses all data stored in the cloud—not just data in transition.\textsuperscript{295} The 1980s notions of data transmission no longer apply so the law should require a search warrant before law enforcement takes possession of any online data. Further, Congress should amend the ECPA to require law enforcement agencies to produce the same kind of reports for seizures of electronic

\textsuperscript{291} Smith Whitepaper, supra note 15, at 3 n.1.
\textsuperscript{294} See Part II.C, supra.
\textsuperscript{295} See Part II.D, supra.
data that they are currently required to produce for wiretaps.\textsuperscript{296} That would allow authorities to monitor compliance with, and the efficacy of, the law.

Third, Congress should create new security breach notification requirements that allow users to assess the exposure, damage, and operational costs of any security failures on the part of a cloud vendor. Currently, forty-five states have breach notification laws that create a confusing patchwork of compliance issues for any cloud provider that operates in multiple states.\textsuperscript{297} Unifying these disparate laws into a single standard would reduce the burden of compliance and make enforcement easier. To protect consumers and businesses from substandard practices, Congress should also charge the National Board of Standards (NSB) to develop minimum reasonable security standards a provider must meet in order to do business across state lines and require detailed disclosure of a provider’s security procedures and measures. And as a part of protecting users’ data-ownership rights, Congress should also use the NSB to develop data recovery standards that users could rely on in the event that their cloud provider fails.

Finally, the ABA should move quickly to establish ethical guidelines for lawyers who use cloud computing services. These guidelines should address document storage, e-mail, collaboration, due diligence for confidentiality, and breach notification related to cloud services. A clear set of guidelines would help protect a lawyer’s clients and allow the lawyer to take advantage cost-effective cloud services that might allow the lawyer give to clients more efficient and cost-effective legal services. Currently, most states leave lawyers without any guidance on proper methods and procedures.


Conclusion

Solid data-ownership boundaries, clear guidelines for law enforcement, clearer penalties for computer crime, and greater cooperation and standardization among cloud providers would go a long way to removing most barriers to wider adoption of cloud computing. The benefits and economies of scale offered by the technology are too great to ignore and leave to the status quo. But cloud providers also need to be responsible with their user’s data. An updated national framework would (1) alleviate problems with data ownership and security by defining clear boundaries, (2) reduce compliance burdens for cloud providers and businesses by standardizing breach notification protocols, and (3) protect consumers and businesses by allowing them to rely on minimum security standards and disclosure requirements.

Current news reports indicate that confidentiality and security concerns trouble the general public less each day. But scientific analysis shows that the public is still very concerned about online security. Giving up confidences should generally be left to individual choice in a system built on “the concept of ordered liberty.” Concerns about the confidentiality and reliability of communications are at least as old as the Republic. But even though new technology presents new challenges, the principles that apply have not changed since the days of the Pony Express. “Plus ça change, plus c’est la même chose”—the more things change, the more they stay the same.

299 Horrigan Memo, supra note 125, at 7; see also Part II.B-C, supra.
301 See Jefferson Letter, supra note 88.
302 RUSH, Circumstances, on HEMISPHERES (Polygram Records 1978).
Figure 1. Software as a Service (SaaS)
Figure 2. Platform as a Service (PaaS)

Software Vendor

Software vendor creates software application

Software Application

Internet

Software vendor sends software application to the cloud via the Internet

PaaS Cloud Vendor

Cloud Vendor Storage

Software application configured for deployment

Software User

Internet

Firewall

Load Balancer

Cloud Vendor Servers

Software application deployed on cloud vendor hardware and scaled according to need

Cloud Services (e.g., .NET, PHP, Java, Python, and the like)
Figure 3. Infrastructure as a Service (IaaS)

Software Vendor

System Specification and Software

Internet

Software vendor sends system specification and software to the cloud via the Internet

IaaS Cloud Vendor

Cloud Vendor Storage

System specification and software configured for deployment

Software deployed on cloud vendor hardware according to system specification

Cloud Vendor Servers

Software User

Internet

Firewall

Load Balancer