Richmond Journal of Law and Technology

Volume 19 | Issue 1 Article 1

2012

Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing

Josiah Dykstra

Damien Riehl

FORENSIC COLLECTION OF ELECTRONIC EVIDENCE FROM INFRASTRUCTURE-AS-A-SERVICE CLOUD COMPUTING

Josiah Dykstra*
Damien Riehl**

I. INTRODUCTION

[1] As cloud computing becomes ubiquitous, the criminal targeting and criminal use of cloud computing is inevitable and imminent. Similarly, the need for civil forensic analyses of cloud computing has become more prevalent. Forensic investigation of cloud computing matters first requires an understanding of the technology and issues associated with the collection of electronically stored information ("ESI") in the cloud. The misuse of the broad term "cloud computing" has caused some confusion and misinformation among legal and technology scholars, leading to a muddied and incomplete analysis of cloud-based discovery issues. Cases and academic analyses have dealt primarily with popular online services such as Gmail and Facebook, but they omit discussions of commercial cloud computing providers' fundamental infrastructure offerings.[1] Even worse, legal analysis about electronic discovery is

* PhD., Computer Science, University of Maryland, Baltimore County, expected 2013; M.S., Information Assurance, Iowa State University, 2004; B.S., Computer Science, Hope College, 2002; B.A., Music, Hope College, 2002. Thanks to Mark Rasch, Alan T. Sherman, Simson Garfinkel, Daniel Dykstra, and Donald Flynn who read prior versions of this Essay and provided helpful comments.

** Attorney with Robins, Kaplan, Miller & Ciresi L.L.P., practicing in business litigation and intellectual property litigation, focusing on cases involving technology. The opinions expressed here are those of the authors; they do not necessarily reflect the views of the firm or its clients. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] *See infra* Part II.A.

largely devoid of authority concerning cloud-computing services.[2] As cloud computing becomes a large and necessary part of our computing existence, policymakers and jurists should carefully analyze how the law should best approach forensic acquisition and analysis of digital artifacts hosted by remote cloud service providers.

[2] In early 2011, Sony was the victim of an online data breach that took down the PlayStation Network.[3] To commit that crime, the intruder used Amazon's public cloud.[4] The FBI investigated the crime, but very little information was made public. For example, neither Amazon nor the FBI would comment on whether the former was served with a search warrant or subpoena.[5] This is likely the first publicly known case of a cloud-related crime, though many more are bound to emerge. Civil cases more frequently address online discovery—most often in the context of services like Gmail or Facebook—but fewer cases have addressed cloud-computing infrastructures like Amazon's Elastic Compute Cloud (EC2),

---

[2] *See generally* H. MARSHALL JARRETT ET AL.,U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115-51(2009) [hereinafter "DOJ MANUAL"], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf. The vendors of the two most popular forensic tools, Guidance EnCase and AccessData FTK, also publish documents describing the electronic discovery process and cases where their products were used; neither mentions cloud forensic acquisition, analysis, or legal precedent. *See generally* GUIDANCE SOFTWARE, ENCASE LEGAL JOURNAL (2011), http://www.guidancesoftware.com/DocumentRegistration.aspx?did=1000017380&id=2525; ACCESSDATA CORP., THE RULES OF DIGITAL EVIDENCE AND ACCESSDATA TECHNOLOGY, http://accessdata.com/downloads/media/Rules_of_Digital_Evidence_and_AccessData_Technology.pdf.

[3] *News: Consumer Alerts*, PLAYSTATION NETWORK, http://us.playstation.com/news/consumeralerts/ (last visited Aug. 22, 2012).

[4] *See* Joseph Galante, Olga Kharif & Pavel Alpeyev, *Sony Network Breach Shows Amazon Cloud's Appeal for Hackers*, BLOOMBERG (May 16, 2011, 4:45 PM), http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html.

[5] *Id.*

Microsoft Azure, or Rackspace.[6] Given cloud computing's intricacies, the courts will likely continue to struggle with the technology's inherent complexities.

[3] This article discusses some challenges involved with electronic discovery and digital forensics arising from cloud computing infrastructure as a service, arguing that the nature of cloud computing challenges the process and product of electronic discovery. We conclude that although existing rules and doctrines—the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and the Fourth Amendment—are appropriately applied to the forensic acquisition and analysis of cloud-based ESI, this technology requires adapting these rules with novel interpretations. We make the following claims: (1) online users have an expectation of the geographic location of their data and thus, the laws protecting that data; (2) cloud providers should not be permitted to execute subpoenas and search warrants on behalf of law enforcement without rigorous guidelines, including challenges to the searches' scope and procedure; and (3) remote forensics of the remote service provider's forum should be governed by the laws of the remote service provider.

[4] Part II defines the technologies and clarifies terms. Part III surveys cases involving cloud forensics, discussing how the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and the Fourth Amendment apply to cloud forensics. Part IV takes a contrasting view, analyzing how parties might undermine cloud-derived evidence.

II. OVERVIEW OF CLOUD TECHNOLOGY

[5] Cloud computing is still an emerging technology, but its use is

[6] *Compare* Equal Emp't Opportunity Comm'n v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 432 (S.D. Ind. 2010) (discussing discovery regarding social media sites), *with* Global Sessions LP v. Travelocity.com LP, No. 6:10cv671, 2012 WL 1903903, at *10 (E.D. Tex. May 25, 2012) (discussing discovery regarding EC2), *and* RealPage, Inc. v. Yardi Sys., Inc., No. CV 11-00690-ODW, 2012 WL 443730, at *6 (C.D. Cal. Feb. 13, 2012) (discussing discovery of generic cloud computing services like Rackspace).

expanding at a blistering pace.[7] In 2011, the United States Government implemented a "Cloud First" policy, requiring that before federal agencies make any new investments, they must evaluate cloud-computing solutions—citing the "considerable benefits to efficiency, agility, or innovation."[8] As such, several government agencies have already implemented cloud solutions,[9] and many more are anticipated to do so in the coming years.[10] Despite this mandate and rush to cloud computing, some policy makers, law enforcement, and forensic investigators do not appear to understand the nuances to investigating incidents and crimes in the cloud, nor do they fully appreciate the implications in civil discovery. Private companies are similarly rushing to cloud computing at a blistering pace.[11] Surveys indicate that most companies use cloud computing,[12] and

[7] *See* Saul Berman et al., *The Power of Cloud*, IBM, 2-3 (Feb. 2012), http://www.ibm.com/cloud-computing/us/en/assets/power-of-cloud-for-bus-model-innovation.pdf.

[8] *See* VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 19 (Feb. 8, 2011), *available at* http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf.

[9] *See, e.g.*, Steve Hoffman, *GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide* (Dec. 1, 2010), http://www.gsa.gov/portal/content/208417; *see also Government Cloud Computing,* CLOUDBOOK, http://www.cloudbook.net/directories/gov-clouds/government-cloud-computing.php (last visited May 31, 2012) (compiling list of government agencies that have adopted cloud computing, including Department of Energy, NASA, National Science Foundation, National Institute of Standards & Technology, and others).

[10] Google's SaaS cloud service has obtained ISO 27001 certification for security techniques. Thomas Claburn, *Google Apps Clears Key Security Hurdle*, INFORMATIONWEEK (May 29, 2012 3:05 pm), http://www.informationweek.com/news/cloud-computing/software/240001126. Microsoft announced a separate cloud product for government: Office 365 for Government. Kirk Koenigsbauer, *Announcing Office 365 for Government: A US Government Community Cloud*, OFFICE 365 (May 30, 2012), http://blogs.office.com/b/microsoft_office_365_blog/archive/2012/05/30/announcing-office-365-for-government-a-us-government-community-cloud.aspx. Both of these developments are sure to rapidly increase government adoption of cloud services.

[11] *See, e.g.*, Berman et al., *supra* note 7.

[12] *See* Smriti Sharma, *74 Percent Companies Using Cloud Services*, GLOBAL SERVICES (Apr. 20, 2012), http://www.globalservicesmedia.com/IT-Outsourcing/Infrastructure-

many use multiple cloud services.[13] Given its rapid adoption, cloud computing has serious legal implications in the United States and around the world. But before analyzing and developing the law, one must first understand the technology.

[6] Legal scholars and practitioners have long made analogies between computer hard drives and filing cabinets.[14] Paul Ohm made this observation: "Warehouses—and even less so filing cabinets—are insignificant containers of information compared to today's hard drives, and the analogy will only become more mismatched over time."[15] To extend Ohm's analogy (warehouses and filing cabinets) to cloud-based data requires the following modification: cut up each document, store each piece in a different locked filing cabinet, and distribute all those cabinets to different warehouses around the world. As Ohm concluded, "Today's technology poses a constitutional puzzle that is different in kind, not just in degree, from the one solved only a few decades ago."[16]

A. Cloud Computing

[7] Cloud computing is a broad, generic term with many proffered

Management/74-Percent-Companies-Using-Cloud-Services/22/6/12123/GS1204209710723.

[13] *See* Meghan Kelly, *86 Percent of Companies Use Multiple Cloud Services, Says Study*, VENTURE BEAT (May 10, 2012), http://venturebeat.com/2012/05/10/cloud-services-data/ (surveying one company's 3,200 customers in 80 different countries).

[14] *See, e.g.*, Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. L. & TECH. 543, 552 (2011) (citing *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12-13 (S.D.N.Y. 1994)); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 550 (2005) (acknowledging the usefulness of treating a computer like a container).

[15] Paul Ohm, *Massive Hard Drives, General Warrants and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 8 (2011).

[16] *Id.*

meanings and definitions.[17] It has infiltrated the vernacular and has been debased in marketing and media. It would be an oversimplification to say that cloud computing refers to anything "in general" other than it is *not* the computing device in your physical possession.[18] The National Institute of Standards and Technology (NIST) provides an often-cited definition of cloud computing that is evolving and non-trivial. A portion of that definition is as follows:

> Cloud computing is 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[19]

[8] Ultimately, cloud computing is a waypoint in decades of technology evolution. Starting with single-user standalone computers and multi-user mainframes, cloud computing's most direct ancestors were utility and grid computing.[20]

---

[17] *See* Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH., 2 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. *See generally* Nicole Galli & Edward Gecovich, *Cloud Computing and the Doctrine of Joint Infringement: 'Current Impact' and Future Possibilities*, 11 J. MARSHALL REV. INTELL. PROP. LAW 673, 676 (2012).

[18] Michael Armbrust et al., *Above the Clouds: A Berkley View of Cloud Computing*, UC BERKELEY RELIABLE ADAPTIVE DISTRIBUTED SYSTEMS LAB, 4 (Feb. 10, 2009), http://inst.cs.berkeley.edu/~cs10/fa10/lec/20/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf.

[19] *See* Mell & Grance, *supra* note 17. This living document has already gone through more than 15 versions. *See* Evelyn Brown, *Final Version of NIST Cloud Computing Definition Published*, NIST (Oct. 25, 2011), http://www.nist.gov/itl/csd/cloud-102511.cfm.

[20] *See* Sourya Biswas, *Cloud Computing vs Utility Computing vs Grid Computing: Sorting the Differences*, CLOUDTWEAKS (Feb. 1, 2011, 7:44 AM),

[9] First, it is important to distinguish between cloud services and cloud computing. Facebook and Gmail are remote cloud *services*, but they are not cloud *computing*.[21] Examples of cloud computing are Amazon Elastic Compute Cloud (EC2), Microsoft Azure, and Rackspace web hosting.[22] "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage.[23] The Internet is one type of cloud.[24] For example, to use Gmail, one need not know the physical location of Gmail's servers. Cloud computing also takes advantage of this definition of a cloud, as it is also a service connected to a network, often the Internet.[25] But cloud computing offers customers additional functionality

http://www.cloudtweaks.com/2011/02/cloud-computing-vs-utility-computing-vs-grid-computing-sorting-the-differences/.

[21] Some authors have mistakenly tied online services to cloud computing. *See, e.g.*, Marc Aaron Melzer, *Copyright Enforcement in the Cloud*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 403, 405 (2011) ("To illustrate this point . . . three sites that can readily be considered examples of SaaS cloud computing: Facebook, the social networking site and number one website by traffic; Yahoo! Mail, the number one webmail provider by accounts; and YouTube, a video sharing site . . . ."). Facebook, Yahoo! Mail, and YouTube do not meet the NIST definition. *See* Mell & Grance*, supra* note 17. Further, they are supported by advertising, not billed to the customer based on their usage.

[22] *See Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2/ (last visited Aug. 7, 2012); *Cloud Services on Windows Azure*, WINDOWS AZURE, http://www.windowsazure.com/en-us/home/scenarios/cloud-services/ (last visited Aug. 7, 2012); *Open Public, Private, and Hybrid Clouds*, RACKSPACE, http://www.rackspace.com/cloud/ (last visited Aug. 7, 2012).

[23] Mell & Grance, *supra* note 17.

[24] Cloud was first used to describe telecommunication networks, where the customer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. *See* Antonio Regalado, *Who Coined 'Cloud Computing'?*, TECH. REV. (Oct. 31, 2011), http://www.technologyreview.com/business/38987/.

[25] *See* Mell & Grance, *supra* note 17, at 3. Cloud computing by definition exposes resources over a network—Public clouds offer these services over the Internet; Private clouds offer services on a private network; such as a private, internal company network;

in the form of raw remote computing resources, such as processing power or data storage, and the ability to provision[26] those resources themselves.[27]

[9] Cloud computing as a utility is actually, though not explicitly, broken down into two forms of service: data-intensive cloud computing (breaking up large computer jobs into smaller subtasks, computing each piece on a different computer)[28] and utility cloud computing (more generic computing resources, such as hard drives and CPUs, which are exposed to customers as a utility).[29] Cloud computing is further broken down into three service models: Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS"), and Software-as-a-Service ("SaaS").[30] Each model represents a different degree of separation between how much infrastructure the customer controls and how much the provider controls.[31] Infrastructure-as-a-Service is the model over which the customer has the

Hybrid clouds link the Internet's public resources with an organization's private resources. *See id.*

[26] "Provisioning" of cloud resources refers to the act of requesting, purchasing, and acquiring the resource so that it is ready for use. This process is often done by filling out a simple form on a management webpage. After the request is received, the storage or computation services can be available to users in as little as a few seconds. *See, e.g.*, *Amazon Elastic Block Store (EBS)*, AMAZON WEB SERVICES, http://aws.amazon.com/ebs/ (last visited Aug. 7, 2012).

[27] *Id.*

[28] *See, e.g.*, Dan Sullivan, *Why Hadoop is the A-list of Big Data*, TOM'S IT PRO (June 8, 2012, 10:17 AM), http://www.tomsitpro.com/articles/hadoop-mapreduce-open_source_software-programming_model-data_management,2-306.html (explaining the software framework behind MapReduce and Hadoop, the technology behind Google's search algorithms, which is illustrative of data-intensive cloud computing).

[29] *See* Sultanulla & Zheng Xuefeng, *Cloud Computing: A Prologue*, INT'L J. OF ADVANCED RES. IN COMPUTER AND COMM. ENGINEERING, Mar. 2012, at 3- 4, *available at* http://www.ijarcce.com/upload/march/Cloud%20Computing%20A%20Prologue.pdf (explaining the framework of Microsoft Azure and Amazon EC2 operating systems, which is illustrative of utility cloud computing).

[30] *See* Mell & Grance, *supra* note 17, at 2-3.

[31] *See* Melzer, *supra* note 21, at 409-11.

most control.[32] For example, when the cloud service is computing resources, the customer has super-user privileges over an entire operating system inside of a virtual machine.[33] The provider owns and controls the rest of the infrastructure, from the hypervisor down to the data center's physical concrete.[34] The two other service models, Platform-as-a-Service and Software-as-a-Service, put more control and responsibility with the provider.[35] Unlike Gmail or Facebook, which provide users with *specific* services, cloud computing is a canvas that programmers can use to create *any* service they choose.[36] This article limits discussion to public clouds rather than private clouds on a company's premises. Few have analyzed the thorny legal issues that arise in electronic discovery of utility cloud computing, which is a topic that Part III explores in more detail.

[10] Four of cloud computing's defining characteristics are particularly important to legal analysis: (1) on-demand self-service; (2) rapid elasticity; (3) location independence; and (4) data replication.[37] First, within the limits defined by the cloud provider, the customer has complete control over the provisioning and de-provisioning of cloud resources,

[32] *See* John Soma et al., *Chasing the Clouds without Getting Drenched: A Call for Fair Practices in Cloud Computing* Services, 16 J. TECH. L. & POL'Y 193, 198-99 (2011) ("In an IaaS Service Model, the user essentially has complete control and responsibility regarding which applications will be deployed in the cloud."). *See generally* Bill Loeffler et al., *What is Infrastructure as a Service*, TECHNET (Sept. 13, 2011, 7:07 AM), http://social.technet.microsoft.com/wiki/contents/articles/4633.what-is-infrastructure-as-a-service.aspx (illustrating and comparing the different types of cloud service models).

[33] *See* Loeffler et al., *supra* note 32.

[34] *See* Paul Rudo, *The Difference Between IaaS, SaaS, and Paas*, ENTERPRISE FEATURES (Aug. 2, 2012), http://enterprisefeatures.com/2011/07/the-difference-between-iaas-saas-and-paas/.

[35] *See id*.

[36] *See generally* Geva Perry, *How Cloud & Utility Computing are Different*, GIGAOM (Feb. 28, 2008, 4:42 PM), http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different/.

[37] *See* Mell & Grance, *supra* note 17, at 2.

which they can do quickly and on-demand.[38] Second, because of this ease and elasticity, customers can cause evidence to appear and disappear at a moment's notice.[39] Third, like other resources on the Internet, the cloud resource's physical location has no bearing on the use or provisioning of those resources, which could exist in one or more data centers around the world.[40] Finally, to provide data reliability and fault-tolerance, cloud providers routinely replicate data on several computers in multiple physical locations.[41] Further, cloud environments typically store data in a distributed file system, breaking single files into pieces that can be stored on multiple independent storage devices, such as hard drives.[42]

---

[38] *See* Yung Chou, *Cloud Computing for IT Pros, Part I: What is Service*, TECHNET BLOGS (Dec. 15, 2010, 4:06 PM), http://blogs.technet.com/b/yungchou/archive/2010/12/15/cloud-computing-concepts-for-it-pros-1-3.aspx.

[39] *See generally* Alberto G. Araiza, *Electronic Discovery in the Cloud*, 2011 DUKE L. & TECH. REV. 8, 35 (2011) (discussing the increased legal risks of deleting ESI under the cloud). *But see* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 675 (3d ed. 2003) (suggesting that the deletion of data is not permanent).

[40] *See* Perry, *supra* note 36 ("Although it is difficult to come up with a precise and comprehensive definition of cloud computing, at the heart of it is the idea that applications run somewhere on the 'cloud' (whether an internal corporate network or the public Internet) – we don't know or care where.").

[41] *See*, *e.g.*, AMAZON WEB SERVICES, AMAZON WEB SERVICES: OVERVIEW OF SECURITY PROCESSES 7 (May 2011), http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf ("Data stored in Amazon S3, Amazon SimpleDB, or Amazon Elastic Block Store (EBS) is redundantly stored in multiple physical locations as a part of normal operation of those services and at no additional charge."); Jeffrey Richter, *Understanding Cloud Storage*, WINDOWS AZURE, http://www.windowsazure.com/en-us/develop/net/fundamentals/cloud-storage/ (last visited Aug. 3, 2012) ("In order to achieve highly available and scalable applications, Windows Azure offers multitenant storage machines within the various Windows Azure data centers. These machines replicate your data ensuring that if one replica fails, others are still viable.").

[42] *See generally* Sean Gallagher, *The Great Disk Drive in the Sky: How Web Giants Store Big—and we mean big—Data*, ARS TECHNICA (Jan. 26, 2012, 9:00 PM EST), http://arstechnica.com/business/2012/01/the-big-disk-drive-in-the-sky-how-the-giants-of-the-web-store-big-data/ (explaining how Google, Microsoft, and Amazon, have adopted distributed file systems and the architecture behind such storage systems).

[11] Under the Stored Communications Act, which governs service providers' voluntary and compelled disclosure of electronic communications and records, cloud computing likely fits the definition of a "remote computing service" ("RCS").[43] When Congress enacted this legislation in 1986, it likely never contemplated anything akin to modern cloud computing.[44] At that time, many businesses could not afford large-scale computation or storage, so data were stored by providers and accessed remotely.[45] Congressional discussion of remote computing services essentially described them as time-sharing services.[46] Those

[43] *See* 18 U.S.C. § 2711(2) (2006) ("the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system"); *see also* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act*, 98 GEO. L.J. 1195, 1212-14 (2010) (examining cloud computing as a remote computing service under the Stored Communications Act).

[44] *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 n.15 (C.D. Cal. 2010); Derek Constantine, Note, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 GA. ST. U. L. REV. 499, 502 (2012).

[45] *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. 19-20 (written testimony of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google Inc.).

[46] *See* H.R. REP. NO. 99-647, at 23 (1986) (citing *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 78 (1986) (statement of P. Nugent, Chairperson, Committee on Computer Systems and Communications Privacy)). Nugent's examples of remote computing services were current for the day, including "the service customer's sales people use terminals to electronically transmit sales order information from geographically dispersed locations to the service vendor's computer center." *Id*; *see also* S. REP. NO. 99-541, at 10 (1986) (describing RCS as "essentially a time-sharing arrangement"). Contrasted from 25 years ago, today's cloud computing environment is fundamentally different, offering more general computing services that customers can quickly and easily provision on demand. The district court in *Viacom International v. YouTube* ruled that YouTube was a remote computing service. 253 F.R.D. 256, 264 (S.D.N.Y. 2008); *see also* Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (holding that "the archive maintained by [the service provider] constitutes 'computer storage,' and that the company's maintenance of this archive on behalf of the City is a 'remote computing service' as defined under the SCA").

systems are distant relatives of today's cloud-computing offerings. By nature of their Internet connectivity and client-server model, cloud providers also provide an "electronic communication service" ("ECS").[47] When selling raw infrastructure resources that include network bandwidth, providers broadly deliver the ability to send or receive any kind of Internet communication.[48]

[12] Cloud-hosted computers can play the same roles in a case as other types of computers.[49] In criminal cases, a cloud-hosted computer could involve or constitute contraband, evidence, fruits, or instrumentalities.[50] Similarly, cloud-hosted computers may contain rich troves of evidence in civil matters.[51] But despite conventional wisdom, seizing a cloud provider's hardware in a criminal matter is often unfruitful.[52] And in a

[47] 18 U.S.C. § 2510(15) (2006) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"). A cloud provider is also likely an "electronic communications system," defined as "any wire, radio, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14) (2006).

[48] Customers that set up services in the cloud may or may not also be an ECS, depending on whether or not they provide the ability to send communications to third parties. *See* Becker v. Toca, No. 07–7202, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008).

[49] *See* State v. Bellar, 217 P.3d 1094, 1110 (Or. Ct. App. 2009) (finding no distinction between data stored on a personal computer and data copied and stored on another medium in the context of privacy rights).

[50] *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2218-20 (2009).

[51] *See, e.g.*, Fed. Trade Comm'n v. First Universal Lending, LLC, 773 F. Supp. 2d 1332, 1342 (S.D. Fla. 2011). *See generally* Steven C. Bennett, *E-Discovery Meets the Cloud*, N.Y. ST. B.J., May 2011, at 45-46 (discussing discovery and a litigator's duties in the context of cloud computing).

[52] Unfortunately, the DOJ Search and Seizure Manual still recommends it. DOJ MANUAL, *supra* note 2, at 70-71; *see also* Liquid Motors, Inc. v. Lynd, No. 3:09–cv-0611–N (N.D. Tex. Apr. 3, 2009) (order ruling that the FBI had reasonable cause to seize

civil matter, such a seizure is often unduly burdensome or logistically impossible.[53] Cases should evolve to contemplate and address the nuances of cloud computing, whose normal operations involve breaking up files and storing them across many servers in many locations.[54] In fact, as part of normal operations, cloud-based data can move easily and transparently to different servers or storage locations.[55] This is not a sufficient argument for a party to request *every* server on *each* of the cloud provider's premises. A forensic examiner analyzing *conventional* computer hardware has the benefit of being able to search for and sometimes recover lost or deleted data still resident on the disk.[56] Although this may be possible with a copy of a virtual machine, it requires additional evidence for a storage service like Amazon's Simple Storage Service (S3).[57] For example, if the provider keeps logs of what files are

computer servers of a cloud-like provider, even though data from other innocent customers were co-mingled with the search warrant's target).

[53] *See* FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 17 (Barbara Rothstein et al. eds. 2007).

[54] Given cloud computing's distributed nature, courts in such cases should move beyond the concept of a server as a singular document repository. *See, e.g.*, United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding seizure of entire computer as contraband in child pornography case); Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) ("[T]he computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."). Unlike *Davis*, where the court observed that "the obvious difficulties attendant in separating the contents of electronic storage from the computer hardware during the course of a search," cloud computing makes this separation natural and convenient. 111 F.3d at 1480.

[55] Jeff Boles, *The Benefits of Cloud-based Storage, Part 2*, INFOSTOR (Nov. 10, 2008), http://www.infostor.com/index/articles/InfoStor-Article-Tool-Template/_saveArticle/articles/infostor/backup-and_recovery/cloud-storage/the-benefits_of_cloud-based.html.

[56] *See, e.g.*, United States v. Gourde, 440 F.3d 1065, 1071 (9th Cir. 2006); *Hay*, 231 F.3d at 635-36; United States v. Crist, 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008); *see also* DOJ MANUAL, *supra* note 2, at 69.

[57] In normal operations, the cloud fabric does this reassembly automatically. If the cloud provider is the criminal defendant or a civil party (not a third party)—or if there is doubt in the trustworthiness of the fabric—then the data's veracity may be suspect.

deleted, who deleted them, and when were they deleted, that could be useful metadata, even if content proves unrecoverable.

[13] In federal criminal cases, the decision of whether to seize hardware also weighs into the choice between a Rule 41 search warrant under the Federal Rules of Criminal Procedure and an Electronic Communications Privacy Act ("ECPA") warrant.[58] While a Rule 41 warrant might be justified for seizing hardware and imaging hard drives on-site, courts have traditionally issued such warrants only for objects physically in the judicial district where the court is located.[59] For ECPA warrants, the statute permits issuance from any court of "competent jurisdiction."[60] The Justice Department's Search and Seizure Manual contains a sample ECPA warrant for e-mail hosted by an ISP[61] as well as a sample Rule 41 warrant for removing computers from the premises.[62]

[14] For civil cases, issuing a subpoena under Rule 45 of the Federal Rules of Civil Procedure is a process similar to that under Rule 41 of the Federal Rules of Criminal Procedure. Rule 45 permits subpoena service in three instances: (1) within the issuing court's district; (2) "within 100 miles of the place specified for the . . . trial, production, or inspection;" or (3) within the state of the trial, production, or inspection.[63] State courts have a limited geographic jurisdiction within their state's borders, so a party cannot enforce extraterritorial subpoenas.[64] As such, a civil party seeking an out-of-state subpoena may choose to initiate an action in a court in the jurisdiction where the hardware is located.

---

[58] *See* United States v. Daccarett, 6 F.3d 37, 46, 53 (2d Cir. 1993); *In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009); DOJ MANUAL, *supra* note 2, at 112, 133-34.

[59] *See* DOJ MANUAL, *supra* note 2, at 84.

[60] 18 U.S.C. § 2703(a) (2006) *amended by* 18 U.S.C. § 2703 (a) (Supp. IV 2009).

[61] DOJ MANUAL, *supra* note 2, at 255-62.

[62] DOJ MANUAL, *supra* note 2, at 241-50.

[63] FED. R. CIV. P. 45(b)(2).

[64] *See* 98 C.J.S. *Witnesses* § 28 (2002) ("Service of a subpoena of a state court outside of the state where it issued is a nullity.").

[15] But because cloud-computing data may be distributed throughout the country or around the world, determining the physical location of such a "production" or "inspection" raises several questions. Is cloud-computing data "produced" at the locations of dozens of servers around the world? If a civil party seeks to "inspect" documents, rather than have them "produced," that party historically would have traveled to a document repository, requiring subpoena service near that repository.[65] With cloud computing, however, does it matter that a requesting party could conceivably conduct such an "inspection" using a computer physically located anywhere in the world, including the venue jurisdiction? Given these quandaries, subpoena service location may be unclear, but the most obvious service location is a cloud service provider's headquarters or principle place of business.

B. Digital Forensics for Cloud Computing

[16] In today's society, ESI is ubiquitous and plays a role in nearly every legal case.[66] Digital forensics uses scientific and proven methods to analyze and interpret ESI to reconstruct events.[67] The forensic examiner is tasked with analyzing ESI to reconstruct a timeline that describes, as best as possible, what happened and when.[68] Although the forensic examiner

[65] *See* FED. R. CIV. P. 34; FED. R. CIV. P. 45(b)(2).

[66] *See* Joseph A. Martin & Christine S. Baxter, *A Practical Guide to Admitting ESI at Trial*, 19 AMERICAN BAR ASSOCIATION BUSINESS TORTS LITIGATION NEWSLETTER, no. 4, Summer 2012, at 2, *available at* http://www.archerlaw.com/files/articles/A%20Practical%20Guide%20to%20Admitting%20ESI%20at%20Trial.pdf.

[67] *See* Brian Carrier, *Defining Digital Forensic Examination and Analysis Tools,* DIGITAL FORENSICS RESEARCH WORKSHOP, Aug. 2002, at 2, *available at* http://www.dfrws.org/2002/papers/Papers/Brian_carrier.pdf. Many people use the term *forensics* in non-criminal contexts because no other term describes digital investigations in non-criminal situations, such as civil cases, intelligence gathering, and internal corporate investigations.

[68] *See* Ovie L. Carroll et al., *Computer Forensics: Digital Forensic Analysis Methodology*, 56 UNITED STATES ATTORNEYS' BULLETIN, no. 1, Jan. 2008, at 4; Christopher Pogue, *Sniper Forensics: GFIRST Edition*, GOVERNMENT FORUM OF

could be asked to analyze single documents or e-mail messages,[69] traditional forensics focuses on analyzing entire hard drives.[70] Cloud computing injects new and non-trivial challenges to this task, including remotely located data, lack of control, layers of complexity, and authenticity. Consider a hypothetical example[71]:

> Alice is a hacker who intends to exploit victims by placing a malicious webpage in the cloud. She uses a vulnerability to exploit the cloud-hosted website of a legitimate company, Buzz Coffee. After hacking into the server, she installs software that infects victims who browse the website. Users complain to Buzz Coffee that they are being infected, so the company seeks to fix the problem and investigate the issue.

[17] This realistic scenario illustrates some of the forensic task's legal issues. If Buzz Coffee owned, operated, and housed the server, then the technical and legal process of acquiring evidence would be routine. Even if Buzz Coffee leased the server from a third party that housed it remotely, it would add very little complexity. But because this scenario involves cloud computing, Buzz Coffee owns no hardware and it might have no idea where any of its data are stored. As discussed in Part III, many conventional questions—such as those of jurisdiction, subpoenas, search warrant issuance and execution, and trustworthy evidence—take on unconventional complexity.

[18] Amazon is unusually open and candid about its internal processes

---

INCIDENT RESPONSE AND SECURITY TEAMS, 34 (2011), http://www.us-cert.gov/GFIRST/presentations/2011/Sniper_Forensics.pdf.

[69] *See* Carroll et al., *supra* note 68, at 3.

[70] *See* Tyler Newby & Ovie L. Carroll, *Rethinking the Storage of Computer Evidence*, 56 UNITED STATES ATTORNEYS' BULLETIN, no. 1, Jan. 2008, at 60.

[71] Josiah Dykstra and Alan T. Sherman, *Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies*, 3 J. NETWORK FORENSICS 1, (forthcoming 2012) (manuscript at 6), *available at* publications.csee.umbc.edu/publications/561/resources/590 (containing the original hypothetical example upon which this example is based).

and support for e-discovery in their cloud offerings known as Amazon Web Services ("AWS").[72] In one risk-management white paper, Amazon describes how it meets customers' needs for electronic discovery, stating that "[c]ustomers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS," and "[u]pon request, AWS may work with customers who require AWS' assistance in legal proceedings."[73] Unlike some cloud providers, Amazon does not explicitly offer services like forensics or incident response assistance.[74] Rather, Amazon and other public cloud providers largely work with parties and law enforcement to the extent required by law.[75]

III. OBTAINING FORENSIC EVIDENCE FROM THE CLOUD

[19] Numerous constitutional and statutory provisions govern searching and acquiring forensic evidence from cloud providers. On the federal level, the analysis focuses on the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, and the Fourth Amendment. In this section, we discuss how each applies to acquiring cloud-based ESI.

---

[72] *See generally Amazon Web Services: Risk and Compliance*, AMAZON WEB SERVICES, 10 (July 2012), http://d36cz9buwru1tt.cloudfront.net/AWS_Risk_and_Compliance_Whitepaper.pdf (addressing whether AWS's cloud services meet e-discovery procedures and requirements).

[73] *Id.*

[74] *E.g.*, Terremark Worldwide, *Investigative Response & Forensics,* http://www.terremark.com/services/security-services/investigative-response.aspx (last visited Aug. 15, 2012) (advertising managed forensics and incident response, whereby the customer pays and the provider performs the work).

[75] *See AWS Service Terms,* AMAZON WEB SERVICES, https://aws.amazon.com/serviceterms/ (last visited Aug. 15, 2012) (stating that Amazon removes content "pursuant to the Digital Millennium Copyright Act or as required to comply with law or any judicial, regulatory or other governmental order or request").

A. Federal Rules of Civil Procedure and Federal Rules of Criminal Procedure

[20] Criminal and civil cases use similar analyses to determine which party is the proper discovery target. Both Federal Rule of Civil Procedure 34 and Federal Rule of Criminal Procedure 16 permit a party to request data "in the responding party's possession, custody, or control."[76] For cloud computing, the "responding party" is usually the cloud provider (as with third-party subpoenas) or a cloud provider's customer.[77] But the question of who has "possession, custody, or control" is more complex.

[21] For example, Dropbox is an online storage service that uses AWS for data storage.[78] Customers negotiate directly with Dropbox, not Amazon.[79] If a Dropbox customer is sued or placed under criminal investigation, the opposing party could potentially request data from Dropbox, Amazon, or both. As demonstrated below, the seeking party's choice of target depends on what data are sought.

[22] When a customer uploads data to the cloud, that customer also arguably transfers the data's custody and possession to the cloud service provider—yet the customer may still retain "control."[80] Depending on the

[76] FED. R. CIV. P. 34(a)(1); *see also* FED. R. CRIM. P. 16(a)(1)(B)(i).

[77] *See generally* FED. R. CIV. P. 34(b)(2); FED. R. CRIM. P. 16(d) (describing the steps required from a responding party).

[78] *See Where does Dropbox store everyone's data?*, DROPBOX http://www.dropbox.com/help/7 (last visited Aug. 15, 2012) (stating that "all files stored online by Dropbox are encrypted and kept securely on Amazon's Simple Storage Service (S3) in multiple data centers located around the United States").

[79] *See generally id.* (noting that Amazon owns Dropbox's physical servers); *DropBox is just a frontend to Amazon S3 with a killer sync feature*, CLOUDIQUITY (Mar. 25, 2012, 12:58 PM), http://www.cloudiquity.com/2012/03/dropbox-is-just-a-frontend-to-amazon-s3-with-a-killer-sync-feature/ (noting that Dropbox employs a frontend sync feature that syncs files stored on Amazon's S3 servers).

[80] *AWS Customer Agreement*, AMAZON WEB SERVICES, at § 8.1, https://aws.amazon.com/agreement/ (last updated Mar. 15, 2012) (stating that "As between [AWS] and [content owner], [owner] or your licensors own all right, title, and

services provided and the parties' contractual relationship, the cloud provider may well act as the customer's agent. Generally, to establish an agency relationship, the agent must generally be authorized to act for the principal, thereby binding the principal by the agent's words or actions.[81] The issue of whether an agency relationship exists is largely fact-dependent.[82] More than for other types of cloud services (e.g., PaaS or SaaS), the agency relationship for parties to an IaaS contract appears clearer because the customer has additional control.[83] For example, AWS customers can instruct the provider to execute automatic actions based on particular events.[84] For instance, the customer can instruct AWS as follows: if a customer's website becomes overwhelmed with too many

interest in and to Your Content . . . including any related intellectual property rights"); *see also Security,* DROPBOX, https://www.dropbox.com/teams/security (last visited Aug. 15, 2012) (specifying that users gain "added control" over their data because Dropbox provides extra security and password protection).

[81] *See* BLACK'S LAW DICTIONARY 70 (9th ed. 2009) (defining "agency" as "[a] fiduciary relationship created by express or implied contract or by law, in which one party (the *agent*) may act on behalf of another party (the *principal*) and bind that other party by words or actions."); HAROLD GILL REUSCHLEIN & WILLIAM A. GREGORY, THE LAW OF AGENCY AND PARTNERSHIP § 1, at 3 (2d ed. 1990); *see also* Asa-Brandt, Inc. v. ADM Investor Servs., Inc., 344 F.3d 738, 743 (8th Cir. 2003) ("[I]n determining whether an agency relationship exists, the question hinged on the principal's right to exercise control over the activities of the agent." (citing Gunderson v. ADM Investor Servs., Inc., No. 99-4032, 2000 WL 1154423, at *2 (8th Cir. Aug. 16, 2000))); United States v. Bonds, 608 F.3d 495, 505 (9th Cir. 2010) (analyzing the Second Restatement's ten factors, noting that the "'essential ingredient . . . is the extent of control exercised by the employer.'" (quoting NLRB v. Friendly Cab Co., 512 F.3d 1090, 1096 (9th Cir. 2008) (alteration in original)).

[82] *See* 2A C.J.S. AGENCY *Generally* § 7 (1972) (noting that determining if an agency relationship exists is a question of fact).

[83] *See, e.g.*, *Sample Technology Statements of Work (SOWs)*, U.S. GEN. SERVICES ADMIN., http://www.gsa.gov/portal/content/133795 (last updated Aug. 22, 2012) (providing samples of IaaS contracts for many different aspects of cloud storage and data protection).

[84] *See AWS Management Console,* AMAZON WEB SERVICES, http://aws.amazon.com/console/#eb (last accessed Aug. 24, 2012) (describing the different cause and effect mechanisms available from AWS).

requests, then AWS should automatically start another virtual machine to assist with the load.[85] This arrangement could be interpreted as one of express actual authority: the customer acts as principal and AWS acts as the customer's agent.[86] If AWS acts as an agent, the customer's fiduciary, then the customer would also arguably have "control" over its cloud-computing data.[87] As such, the customer could be required to produce the cloud-computing data that it controls.

[23] Where discovery requests and subpoenas are issued to cloud providers directly and without reference to whether the provider "controls" that data, those situations require a different analysis. To discuss what data are in the cloud provider's possession, custody, or control, one should first understand what data might be available.[88] Infrastructure-as-a-Service can be viewed as a multi-layered cake, with each layer independently comprising part of the cloud service. The cake's top layer contains the customer's data and applications, which Internet users may utilize as a webpage or database.[89] These data are the first that may be available and by definition of IaaS, the data are owned and controlled by the customer.[90] The next layer is the guest virtual machine,

[85] *See id.* (describing the "Elastic Beanstalk" feature which "handles the details of capacity provisioning, load balancing, auto-scaling, and application health monitoring").

[86] *See* FTC v. First Universal Lending, LLC, 773 F. Supp. 2d 1332, 1347-49 (S.D. Fla. 2011) (discussing a party's data on servers owned by cloud service Salesforce, which constituted the "backbone" of a party's business).

[87] *Compare AWS Customer Agreement*, *supra* note 80 (describing customer control in AWS services), *with* C.J.S. AGENCY, *supra* note 82 (describing the agency relationship).

[88] The complete set of forensic data available to a requestor is categorically unknown. The public cloud providers have thus far withheld their capabilities, possibly because they are protecting the proprietary implementation that gives them competitive advantage. We speculate about data that are likely available, but cannot speculate about the provider's practical ability to collect these data.

[89] *See* Loeffler et al., *supra* note 32.

[90] *See Infrastructure as a Service (IaaS)*, U.S. GEN. SERVICES ADMIN., www.gsa.gov/iaas (last updated July 5, 2012).

which in IaaS is also owned and controlled by the customer.[91] The cake's third layer is the hypervisor: special software that runs on a provider's computer (the host), allowing many virtual machines to run independently on a single physical machine.[92] Below the physical machine is the distributed array of storage disks.[93] The cake's base is the computer networking that interconnects the components, providing high bandwidth to the Internet.[94]

[24] To date, the major cloud providers have not yet released their policies regarding their responses to civil or criminal requests, nor have they described the types of records and data that they will make available.[95] But cloud providers do have data that could prove useful in criminal and civil matters. For example, cloud providers maintain data related to subscriber information and billing records.[96] Because customers are billed based on their usage, records relating to service usage should

[91] *See Infrastructure as a Service*, CDW, 2 (2011), *available at* http://www.edtechmagazine.com/higher/sites/edtechmagazine.com.higher/files/108289-wp-inf_service_df.pdf; *Information Supplement: PCI DSS Virtualization Guidelines*, PCI SECURITY STANDARDS COUNCIL, 23 (June 2011), https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

[92] Francoise Gilbert, *Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking Off*, 14 No. 6 J. INTERNET L. 1, Dec. 2010, at 17, 19; PCI SECURITY STANDARDS COUNCIL, *supra* note 91, at 7.

[93] *See* Loeffler et al., *supra* note 32; PCI SECURITY STANDARDS COUNCIL, *supra* note 91, at 6.

[94] *See* Loeffler et al., *supra* note 32; PCI SECURITY STANDARDS COUNCIL, *supra* note 91, at 6.

[95] *See* Ashish S. Prasad, *Cloud Computing and Social Media: Electronic Discovery Considerations and Best Practices*, THE METROPOLITAN CORPORATE COUNSEL, Feb. 2012, at 26, 27, *available at*: http://www.metrocorpcounsel.com/articles/17454/cloud-computing-and-social-media-electronic-discovery-considerations-and-best-practic; *cf.*, John Soma, et al., *supra* note 32, at 220-21.

[96] *See* Joshua S. Parker, Note, *Lost in the Cloud: Protecting End-User Privacy in Federal Cloud Computing Contracts*, 41 PUB. CONT. L.J. 385, 396-97 (2012).

also be available.[97] Beyond these obvious requests, providers often keep other data for some time. A provider uses connection information (sometimes called NetFlow records), to record an Internet communication's two endpoints; this non-content data can be useful as a historical record.[98] When a customer wishes to procure or manage cloud services, that customer typically visits a special website to manage those actions.[99] That website and its underlying components may also be an attractive source of forensic evidence. The provider might be able to produce logs showing successful and unsuccessful logins, the logins' IP addresses and geographic origins, and their time and date. If services can be provisioned programmatically, then similar logs may be available.

[25] Although the cloud system's operation may not require *humans* to know where data are located (e.g., server or data center), the underlying *infrastructure* must know that information.[100] The provider may record system logs that describe where the data are; who created them; and when they were created, modified, or deleted. In sum, no universal template currently exists for parties and law enforcement seeking cloud data; often, they do not know what they can or should ask for. Moreover, the data that cloud service providers house can be as unique as the cloud service providers themselves.

[26] Regarding IaaS, data inside a customer's virtual machine (e.g., webpages) are hidden even from the provider unless the customer makes

[97] *See id*; *see also Architecture for Managing Clouds*, DISTRIBUTED MANAGEMENT TASK FORCE, 39 (June 18, 2010), http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf.

[98] *See* Jamie Epstein, *Get in the Know, NetFlow is the Way to Go*, TMCNET.COM (July 30, 2012), http://netflow.tmcnet.com/articles/300888-get-the-know-netflow-the-way-go.htm.

[99] *See* Loeffler et al., *supra* note 32.

[100] *See* DISTRIBUTED MANAGEMENT TASK FORCE, *supra* note 97, at 26.

that data available.[101] The cloud provider, whose ownership and responsibility extend to the hypervisor and below, could access the computer files that make up the virtual machine and when responding to discovery, they could provide a copy of that virtual machine.[102] Providers are also capable of collecting content and non-content forensic evidence in their possession, custody, and control. For example, they could collect network packet captures of all ingress and egress network traffic from their cloud, they could collect logs showing the data's physical storage locations, and they have billing data about the provisioning and usage of cloud resources.[103]

[27] Providers' contractual language with their customers will

[101] *See* Wely Lau, *Comparing IAAS and PAAS: A Developer's Perspective*, ACLOUDYPLACE (Jan. 13, 2012), http://acloudyplace.com/2012/01/comparing-iaas-and-paas-a-developers-perspective/.

[102] *See* Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NAT'L INST. OF STANDARDS & TECH., 12, 18 (Dec. 2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[103] *See id.* at 12, 20-21 (explaining that cloud service providers have access to a lot of information that the user does not have access to). The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires telecommunications carriers to assist law enforcement in performing electronic surveillance pursuant to court orders. 47 U.S.C. §§ 1001-1010 (2006). However, the term "telecommunications carrier" does not include "persons or entities insofar as they are engaged in providing information services." 47 U.S.C. § 1001(8)(C)(i). The law does not require cloud providers to provide real-time interception capabilities. In a statement before the House Judiciary Committee, the FBI and others identified this as a shortcoming. *See, e.g.*, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary,* 112th Cong. 23-24 (2011) (statement of Susan Landau, Fellow at the Radcliffe Institute for Advanced Study at Harvard University); *FBI - Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, FEDERAL BUREAU OF INVESTIGATION (Feb. 17, 2011), http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies (posting the testimony of Valerie Caproni, General Counsel to the Federal Bureau of Investigation, before the Subcommittee on Crime Terrorism, and Homeland Security).

determine the extent to which those customers may access these data.[104] To complicate matters, providers possess some data over which their customers may not have access (e.g., infrastructure logs), as well as other data over which the providers may not have control (e.g., customer's data).[105]

[28] Preservation is an essential tool in electronic discovery, particularly with data that is highly volatile or elastic.[106] For criminal matters, compelling a provider to preserve a snapshot of potential evidence requires a very low bar.[107] For civil matters, the bar for obtaining forensic data is higher and more time-intensive, so civil parties who require such ephemeral data are wise to start the process of acquisition quickly.[108]

[29] If they do not have one already, cloud providers should have some mechanism for preservation. On one hand, providers have an advantage in preserving large data volumes since they advertise broad storage

[104] *See, e.g.,* Flagg v. City of Detroit, 252 F.R.D. 346, 354 (E.D. Mich. 2008) (the court ruled that text messages held by a provider were subject to the city's control, given that the city had some contractual right of access to the data).

[105] *See* Jansen & Grance, *supra* note 102, at 20-21.

[106] Erik Harris, Note, *Discovery of Portable Electronic Devices*, 61 ALA. L. REV. 193, 197, n.24 (2009); *cf.* Cameron G. Shilling, *Electronic Discovery: Litigation Crashes into the Digital Age,* 22 LAB. L., 207, 227 (2007).

[107] ECS and RCS providers "upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" for 90 days, which can be renewed for an additional 90 days. 18 U.S.C. § 2703(f) (2006). Section 2704 describes how a governmental entity, in a subpoena or court order, may order the provider to create a backup copy of the contents of the communications. 18 U.S.C. § 2704(a) (2006).

[108] *See* Shilling, *supra* note 106, at 214 (explaining that counsel should discuss E-discovery issues early on in the litigation process); Justin P. Murphy, *E-Discovery in Criminal Matters—Emerging Trends & The Influence of Civil Litigation Principles Post-Indictment E-Discovery Jurisprudence*, 11 SEDONA CONF. J. 257, 259, 262-64 (2010) (pointing out that electronic discovery for criminal matters do not have to follow the much more strict discovery requirements under the Federal Rules of Civil Procedure).

resources.[109] Additionally, IaaS resources such as virtual machines inherently permit providers to take snapshots of the running machines at any time.[110] On the other hand, providers may not be able to prevent their customers from de-provisioning resources or deleting data. Consider the following example, where current cloud practices could inhibit preservation:

> Cloud resources, such as virtual machines, are launched using a user's private key. A hacker steals a key from a legitimate user, launches hundreds of machines that flood a popular website, and takes it offline. The opposing party may request data from the legitimate user, seeking activity logs to show who launched the machines, as well as copies of the machines themselves. But the legitimate user may have no logs to produce and the attacker may have tried to cover its tracks by deleting the hundreds of malicious machines.

In traditional digital forensics, investigators would create a mirror image of a hard drive that the examiner can then search for deleted files.[111] Tragically, although cloud providers likely know *when* files in their storage array are deleted and although they may have logs to prove it, they probably lack the ability to *recover* deleted files or to produce complete hard disk images.[112]

---

[109] *Cf.* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 262 (S.D.N.Y. 2008) (ruling that the need for 12 terabytes of data outweighed the expense and burden of production).

[110] *See* Shathabheesha, *Virtualization Security in Cloud Computing,* INFOSEC INSTITUTE (June 21, 2012), http://resources.infosecinstitute.com/virtualization-security-cloud-computing/ (explaining that anyone with access to the host disk files on a virtual machine can create a snapshot).

[111] *See* Franz J. Vancura, *Using Computer Forensics to Enhance the Discovery of Electronically Stored Information,* 7 U. ST. THOMAS L.J. 727, 728-29 (2010).

[112] Microsoft Azure's service level agreement reads "You're responsible for backing up the data that you store on the service . . . . Data that is deleted may be irretrievable." *Microsoft Services Agreement*, MICROSOFT, http://windows.microsoft.com/en-US/windows-live/microsoft-service-agreement (last visited Aug. 27, 2012).

[30] Because cloud computing is so elastic, its corresponding data are often ephemeral.[113] While some courts have noted that ephemeral data "are not discoverable in most cases,"[114] some courts have held that in certain cases, ephemeral data, such as random access memory (RAM) data, are discoverable.[115] At least one court has affirmed the discoverability of IP addresses.[116] In the cloud, both RAM and IP addresses are potentially fleeting and quickly inaccessible.[117] Although a civil party must preserve evidence when it reasonably anticipates litigation,[118] the Federal Rules of Civil Procedure also relieve parties of the duty to preserve if the data are "lost as a result of the routine, good-faith operation of an electronic information system."[119] At a minimum, cloud providers are more likely to retain data about when resources are

[113] *See Amazon Elastic Compute Cloud Getting Started Guide,* AMAZON WEB SERVICES, 5 (Mar. 11, 2008), http://ec2dream.webs.com/AWS-Management-Console.pdf.

[114] H. JAMES F. HOLDERMAN ET AL., SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM 14 (2009), *available at* http://www.ilcd.uscourts.gov/Statement%20-%20Phase%20One.pdf (listing categories of data "not discoverable in most cases," including hard drives' "deleted" or "unallocated" data, RAM, "ephemeral data," temporary files, cache frequently updated metadata, duplicative backup data, and other ESI requiring "extraordinary affirmative measures"); *see also* Phillips v. Netblue, Inc., No. C-05-4401 SC, 2007 WL 174459, at *2-3 (N.D. Cal. Jan. 22, 2007) (holding a party's argument that hyperlinks should have been preserved was absurd).

[115] *E.g.*, Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 453 (C.D. Cal. 2007); Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 524 (D. Md. 2010) ("[t]he general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and metadata"); Tener v. Cremer, 931 N.Y.S.2d 552, 555-57 (N.Y. App. Div. 2011) (remanding for determination of several questions, including the data's current availability, custodians, and cost for retrieval).

[116] *See Columbia Pictures*, 245 F.R.D. at 451.

[117] *See generally* Conrad J. Jacoby, *E-Discovery Update - Discovery of Ephemeral Digital Information*, LAW AND TECHNOLOGY RESOURCES FOR LEGAL PROFESSIONALS (Jul. 27, 2007), http://www.llrx.com/columns/fios19.htm (explaining how RAM is constantly rewritten and therefore a fleeting storage space).

[118] *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

[119] FED. R. CIV. P. 37(e).

provisioned and de-provisioned since those activities directly determine a customer's bill.[120]

[31] Contracts between the cloud provider and customers often detail such issues of ownership.[121] Clear contractual provisions can help to avoid later litigation and expense. Where contracts do not sufficiently discuss ownership, however, parties must look to case law. For example, the court in *Flagg v. City of Detroit* found that the city had a contractual right to text messages held by a third party provider.[122] The *Flagg* court did not address the ownership of other data, such as the provider's logs.[123] For discovery requests, subpoenas, or search warrants, any requesting party would be wise to determine what data is in what party's possession or custody, whether the provider, the customer, or both.

---

[120] *See generally* Matthew Wachs et al., *Exertion-based billing for cloud storage access*, PROCEEDINGS FOR THE 3RD USENIX WORKSHOP ON HOT TOPICS IN CLOUD COMPUTING (HOT CLOUD '11), (June 14-15, 2011), *available at* http://www.pdl.cmu.edu/PDL-FTP/CloudComputing/hotcloud11-final62.pdf (discussing the different rates for charging cloud customers depending on their amount or usage).

[121] Amazon Web Services has such an agreement. *See AWS Customer Agreement*, *supra* note 80. This contract defines "content" as "software (including machine images), data, text, audio, video, images or other content." See *id.* at § 14. In Section 8.1, Amazon clams "no rights under this Agreement from you or your licensors to Your Content, including any related intellectual property rights." *Id.* at § 8.1. The document defines "Service Offerings" as "the Services (including associated APIs), the AWS Content, the AWS Marks, the AWS Site, and any other product or service provided by us under this Agreement." *Id.* at § 14. In Section 8.4, Amazon clams that "we or our affiliates or licensors and reserve all right, title, and interest in and to the Service Offerings." *Id.* at § 8.4. In other words, the customer explicitly owns their virtual machines, and does not own the IP address, hardware, or cloud-hosting infrastructure. Microsoft contracts contain similar language. *See Microsoft Services Agreement*, *supra* note 112 ("Except for material that we license to you, we don't claim ownership of the content you provide on the service. Your content remains your content."). But unlike Amazon's agreement, Microsoft's Service Agreement does not define "content." *See id.*

[122] 252 F.R.D. 346, 354 (E.D. Mich. 2008).

[123] *See generally id.* (discussing the discoverability of text messages).

[32] Determining jurisdiction in cloud-computing environments is unlike any prior jurisdiction analysis. Even more than websites, cloud computing is neither jurisdictional nor multi-jurisdictional. It is non-jurisdictional in that physical geography frequently does not matter. Even for existing cases discussing online data, those cases almost exclusively revolve around websites.[124] Although online services such as Facebook and Gmail frequently comply with discovery requests, those cases rarely, if ever, discuss the nature of the services' back-end geographic location and the locations of the resultant data.[125] In the cloud, the issue compounds since data are likely stored in several jurisdictions and possibly even across international borders among countries with conflicting laws. For example, in one criminal case, the defendant was tried in California because she was accused of violating a social networking site's terms of service and the site's owner was located in California.[126] Courts frequently apply the "effects test" for personal jurisdiction, which is based on "(1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered—and which the defendant knows is likely to be suffered—in the forum state."[127] Under this framework, one would expect most cloud-based litigation to occur in the cloud customer's forum state.[128] The effects test assumes that most often, the crimes, infringements, or torts are committed against the data owners in their forum state without any intent to cause harm in the forum state of the data.[129]

---

[124] *See, e.g.*, Facebook v. Connectu LLC, No. C 07-01389 RS, 2007 U.S. Dist. LEXIS 61962 *10-22 (N.D. Cal. Aug. 13, 2007) (discussing jurisdiction as relates to the Plaintiff's website).

[125] *See, e.g.*, *id.* at *14-15.

[126] United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009).

[127] Core-Vent Corp. v. Nobel Indus. AB, 11 F.3d 1482, 1486 (9th Cir. 1993) (citing Calder v. Jones, 465 U.S. 783 (1984)).

[128] *See generally Facebook*, 2007 U.S. Dist. LEXIS at *14-15 (explaining how jurisdiction has typically been evaluated by the courts regarding the effects test).

[129] *See, e.g.*, Brayton Purcell LLP v. Recordon & Recordon, 606 F.3d 1124, 1128 (9th Cir. 2010).

[33] For crimes involving cloud computing, following Rule 18—that "the government must prosecute an offense in the district where the offense was committed"[130]—is not straightforward. Where the object of the crime is the cloud, a criminal case could potentially be tried in one of four venues: that of the perpetrator, the cloud provider, the cloud customer, or the online data location. Cloud service providers may dictate the venue in their contract, but that may not be binding criminally.[131] Barring a contractually chosen venue, 18 U.S.C. § 3237 allows for criminal offenses committed in one district to "be inquired of and prosecuted in any district in which such offense was begun, continued, or completed."[132] Courts have described the determination of a proper venue "as a substantial contacts rule that takes into account a number of factors—the site of the defendant's acts, the elements and nature of the crime, the locus of the effect of the criminal conduct, and the suitability of each district for accurate fact finding."[133] In cloud-based crimes, none of these factors creates an obvious choice. Any of those four locations could arguably be a proper venue.

[34] Cloud computing and most other web services exist without deference to geographical location.[134] Customers generally have a reasonable expectation of location for their data; they generally believe that if they are using a service provided by a U.S. company, then their data

[130] FED. R. CRIM. P. 18.

[131] *See, e.g.*, *Cisco Connect Cloud Terms of Service*, CISCOCONNECTCLOUD, http://ciscoconnectcloud.com/ui/ustatic/termsofservice/1.0.0/termsofservice-en-US.html (last visited August 19, 2012) (providing an example of a contract in which the provider dictates choice of venue).

[132] 18 U.S.C. § 3237 (2006).

[133] United States v. Beddow, 957 F.2d 1330, 1335 (6th Cir. 1992) (quoting United States v. Williams, 788 F.2d 1213, 1215 (6th Cir. 1986)).

[134] *See generally* Mell & Grance, *supra* note 17, at 2 (describing the location independence of resources as an essential characteristic of cloud computing).

reside in the United States.[135] Looking at their providers' top-level domain names, users may assume that data stored by "www.state.md.us" is located in the United States, while data stored by "mail.ru" is located in Russia.[136] Most service-level agreements for online services do not specify the location where data will be stored.[137] Absent any reason to believe otherwise,[138] customers and end-users will make assumptions about the data's location, as well as the laws governing it.

[35] In criminal cases, several vehicles can compel data from a provider. As with any other data, 18 U.S.C. § 2703 offers prosecutors five mechanisms to obtain certain information from a provider: (1) Subpoena; (2) Subpoena with prior notice to the subscriber or customer; (3) § 2703(d) court order; (4) § 2703(d) court order with prior notice to the subscriber or customer; and (5) Search warrant.[139]

[36] The Department of Justice prefers using "a subpoena or other less intrusive means to obtain evidence from disinterested third parties, unless use of those less intrusive means would substantially jeopardize the availability or usefulness of the materials sought."[140] Losing the availability of data is of paramount concern given the cloud's elasticity. Regardless of the vehicle used, some data may be in the provider's

---

[135] *See* Joseph A. Schoorl, Note, *Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls*, 80 GEO. WASH. L. REV. 632, 648 (2012) (stating that cloud users are generally unaware that their data are transferred across national borders).

[136] The Internet Assigned Numbers Authority (IANA) assigns top-level domain names based on the International Organization for Standardization (ISO) 3166–1 alpha-2 country codes. The United States is assigned .us and Russia is assigned .ru. *See ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)*, ICANN, http://www.icann.org/en/icp/icp-1.htm (last visited Sept. 20, 2012).

[137] *See, e.g.*, CISCOCLOUDCONNECT, *supra* note 131.

[138] Amazon Web Services, for example, allows customers to specify the geographic region where data is stored. *See AWS Customer Agreement*, *supra* note 80.

[139] 18 U.S.C. § 2703(a)-(d) (2006).

[140] *See* DOJ MANUAL, *supra* note 3, at 111.

possession, custody, or control, whereas other data may be in the cloud customer's possession, custody, or control. To further complicate matters, the Stored Communications Act has been interpreted to prohibit a provider from disclosing user content in response to a civil subpoena.[141] This decision provides drastically different protections for data storage in an ECS versus a provider of RCS, where 18 U.S.C. § 2703(b) allows a cloud provider, acting as a provider of RCS, to disclose the contents of an account used for remote storage without a warrant and without notifying the customer or subscriber.[142] One scholar, Orin S. Kerr, has suggested that this disparate treatment is unconstitutional.[143]

[37] Another issue to consider is time. Rule 45 of the Federal Rules of Civil Procedure does not specify a minimum time period within which a responding party must comply with a subpoena.[144] Typically, the issuing party will permit the responding party to comply in ten to thirty days, except where the issuing court's local rules dictate another minimum period for compliance.[145] Given the ease with which cloud data can be either be overwritten or destroyed, as well as providers' lack of evidence preservation mechanisms, the threat of spoliation dramatically

[141] *See* Flagg v. City of Detroit, 252 F.R.D. 346, 350 (E.D. Mich. 2008) ("[The Stored Communications Act] lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to subpoena or court order.").

[142] *See* 18 U.S.C § 2703(b) (2006).

[143] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1029 (2010).

[144] *See generally* FED. R. CIV. P. 45 (discussing the form in which documents must be produced). Courts, however, "may specify conditions for the discovery." FED. R. CIV. P. 45(d)(1)(D).

[145] *See* David J. Lender et al., *Federal Practice: Responding to a Subpoena*, PRACTICAL LAW COMPANY, 7 (2010), *available at* http://www.weil.com/files/Publication/925ba5e1-3ebb-4758-8e83-a1424fdff940/Presentation/PublicationAttachment/e8247337-b86d-4df9-b01b-a953f20b0545/10.18.10-Federal%20Practice%20Responding%20To%20A%20Subpoena%20(1-503-1741)%20(2)%20(2).pdf.

increases.[146] One solution is to require faster subpoena compliance.[147] But the difficulties with this approach are that it would require human intervention at the cloud provider and it does not scale.[148] Another solution is empowering data owners and investigators to gather forensic evidence themselves.[149] This option would shift the burden from the provider (who lacks monetary or legal incentive to quickly comply) to the parties themselves (who have every incentive to collect evidence quickly and inexpensively).

B. Fourth Amendment

[38] Search and seizure of evidence regarding crimes committed in or against the cloud should be valid under the Fourth Amendment.[150] This

---

[146] *See* THE SEDONA CONFERENCE, *The Sedona Conference Commentary on Cloud Computing (Draft)* 28-31 (The Sedona Conf. Working Paper Grp. 1, 2011).

[147] *But see* Erin E. Rhinehart, *Civil Subpoenas in Federal Court: Complying with Third-Party Subpoenas*, AMERICAN BAR ASSOCIATION (2012), http://apps.americanbar.org/litigation/committees/pretrial/articles/0923_civil-subpoenas-2.html (discussing what is considered a "'reasonable time to comply'" under the current version of Rule 45). The Rule 45 "reasonable time" requirement may prove antagonist to the goal of faster subpoena compliance.

[148] *See* Meera Unnithan Sossamon, *Subpoenas And Social Networks: Fixing The Stored Communications Act In A Civil Litigation Context*, 57 LOY. L. REV. 619, 642-43 (highlighting the unreasonably high costs and expenses associated with cloud computing providers' subpoena compliance); *see also* Steven S. Gensler, *The Intersection of Facebook and the Law: Symposium Article: Special Rules for Social Media Discovery?*, 65 ARK. L. REV. 7, 35 (2012) (addressing a discussion held by the Discovery Subcommittee over whether a "detailed rule" regarding "when the duty to preserve is triggered and what must be preserved" is necessary, or whether that rule would be too limiting given rapid developments in technology).

[149] This area is being actively explored by one of this article's authors.

[150] *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *see also* David J. Goldstone & Daniel B. Reagan, *Practice Tips: Social Networking, Mobile Devices, and the Cloud: The Newest Frontiers of Privacy*

topic has become a focal point of discussion over recent years; scholars have carefully looked at the interplay between privacy and cloud computing.[151]

[39] For simplicity, we will assume that cloud-computing customers have a reasonable expectation of privacy for their data.[152] We also proceed under the current case law applying the Fourth Amendment to online data.[153] Therefore, under *Katz v. United States* and its progeny, obtaining cloud data constitutes a search and violating the reasonable expectation to privacy implicates the Fourth Amendment.[154] More difficult are the issues surrounding warrant execution for cloud data.[155]

[40] Warrants for web-based e-mail can specify particular senders, recipients, and timeframes, thereby preventing the unnecessary production of the entire e-mail corpus.[156] In IaaS, the warrant may similarly narrow

Law, 55 B.B.J. 17, 20-21 (2011) (noting that the "court held that [the defendant] had a reasonable expectation of privacy in his emails stored by the ISP, finding that emails are subject to the same Fourth Amendment protections as letters and phone calls" (citing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010))).

[151] *See*, *e.g.*, Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 594-98 (2010); David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless*, 25 BERKELEY TECH. L.J. 621, 638, 642-47 (2010).

[152] *See* Couillard, *supra* note 50, at 2205-06 ("[U]sers expect their information to be treated the same on this virtual cloud as it would be if it were stored on their computer, phone, or iPod.").

[153] *See* R. Bruce Wells, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 U. PA. J. CONST. L. 223, 225-29 (2009) (featuring a proposal to protect online data under an entirely new doctrine); *see also* Couillard, *supra* note 50, at 2205.

[154] Katz v. United States, 389 U.S. 347 (1967)*; see also* Wells, *supra* note 153, at 226-27.

[155] *See generally* Barnhill, *supra* note 151 (discussing reasonable expectation of privacy in the workplace and in data migrating to the cloud).

[156] *But see* Constantine, *supra* note 44, at 518-520 (discussing the dilemma of determining whether a part of the e-mail should be considered "content" or "non-content", and the implications for a search warrant based on this distinction).

the search for data by filename, creation time, or author.[157] Recently Kerr criticized the *ex ante* regulation of computer search and seizure.[158] Despite the potential for an unprecedented and overwhelming volume of ESI from cloud crimes, search warrants in these cases have a unique opportunity to address the particularity issue often associated with digital searches. Unfortunately, because cloud providers are often opaque about their infrastructure, it would be impossible or unwise for the warrant to specify the search strategy or approach of execution.[159] With a basic understanding of cloud-computing technology, courts should decline to impose limits as conditions on issuing cloud-targeted warrants.

[41] Today, most search warrants for online data are served upon providers, who subsequently execute them.[160] The provider's legal

[157] *See, e.g.*, Marlo Arredondo Aff. for Search Warrant 2, Aug. 7, 2008. *But see* Kerr, *supra* note 14, at 543-48 (discussing the ability for users to alter these characteristics, making certain data nearly impossible to find). Given the nature of digital evidence, this does not overcome the need to scan the container for the evidence. Just as one would leaf through a filing cabinet looking for a particular document, so too must the investigator scour the computer looking for the particular file. Unfortunately, distributed cloud data may require the leafing through many filing cabinets in many warehouses in many locations, where data is co-mingled with other users' data. *Id.* at 576-77 (including a discussion on the plain view doctrine).

[158] Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) ("[Arguing] that ex ante regulation of computer warrants is both constitutionally unauthorized and unwise.").

[159] *See* Constantine, *supra* note 44, at 501 ("Considering the expansive nature of the terms of Google's general service agreement and assuming consumers actually read the agreement rather than blindly clicking 'agree,' users may wonder what level of privacy their files will have if uploaded or sent through one of Google's services."); *see also* Ari Schwartz et al., *Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues*, 1 J.L. & POL'Y INFO. SOC'Y 597, 597 (2005) ("[I]t is sometimes hard to determine what a specific provider's policy is, especially with respect to deletion of mail from inactive accounts or deletion of older mail from active accounts."). *But see* Kerr, *supra* note 14, at 565 ("The Framers of the Fourth Amendment included a particularity requirement to disallow general searches: all warrants must describe *ex ante* the particular place to be searched and the particular person or thing to be seized.").

[160] *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Winston Maxwell & Christopher Wolf, *A Global Reality: Government Access to Data in the Cloud*, HOGAN

authority to execute a warrant comes from both statutory and case law.[161] The practical reason is also germane: law enforcement officers have neither the resources nor expertise to execute warrants surrounding cloud computing.[162] This is consistent even with traditional search warrants. When officers go to an office building looking for evidence, they do not ask the occupants to locate that evidence. They know what they are looking for, so it is more efficient for them to do the search, rather than relying on the occupant who lacks incentive to be thorough. For cloud computing, however, when the cloud provider executes the warrant at the bequest of law enforcement, it may become the government's agent.[163]

LOVELLS, 4 (May 23, 2012), *available at* http://www.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf (last updated July 18, 2012).

[161] *See, e.g.*, 18 U.S.C. § 3105 (2006) ("A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution."); 18 U.S.C. § 2703(g) (2006) ("Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service."); United States v. Bach, 310 F.3d 1063, 1066-67 (8th Cir. 2002) ("The Fourth Amendment does not explicitly require official presence during a warrant's execution, therefore it is not an automatic violation if no officer is present during a search.").

[162] *See* Couillard, *supra* note 50, at 2217.

[163] *See* Lugar v. Edmondson Oil Co., 457 U.S. 922, 953 (1982); People v. McKinnon*,* 500 P.2d 1097, 1106 (Cal. 1972); People v. Scott*,* 117 Cal. Rptr. 925, 926 (Cal. Ct. App. 1974). In *United States v. Richardson*, the Fourth Circuit has held that AOL was not acting as an agent for the government when it uncovered and reported child pornography in a customer's e-mail. 607 F.3d 357, 366-67 (4th Cir. 2010). This activity was not done at the government's request, but reported pursuant to an unrelated statute that requires mandatory reporting of suspected violations of child pornography regulations. *Id.* Professor Steven R. Morrison has suggested that ISPs be treated as state actors for any search of user's e-mail. *See* Steven R. Morrison, *What the Cops Can't Do, Internet*

Cloud providers may also look for ways to empower customers and law enforcement to acquire forensic data through self-help. This capability is admirable and would free the provider from the burden of doing all the work. It would also be an attractive feature to potential security-minded clients. Regardless of who does the search, whether the provider or law enforcement, this approach raises two new questions, which apply equally to civil litigation: first, where can the search be done, and second, what law applies?

C. Jurisdictional Difficulties and Costs of Implementation

[42] Consider an example that illustrates this problem. Imagine that a cloud provider incorporated in California has a data center in Virginia. A Washington, D.C. court issues a warrant for data residing in the Virginia data center. A New York resident owns the data. If the provider executes the search, it does so from a computer terminal in California. The provider also provides the FBI with access to search remotely from their offices in D.C. We propose that where the search is done (inside the United States) is immaterial and that California law should control. The interconnected, networked nature of a national or global company makes *where* the search is conducted irrelevant. Even if the provider physically executes the search in California, it still accesses the data remotely, flowing across many interstate networks to the Virginia data center. It follows, however, that the location of the provider (in this example, incorporated and governed by California law) should be the operative jurisdiction, regardless of where the search occurs.

[43] Upon execution of a warrant, the cost of cloud-based ESI collection and production could be expensive.[164] The situation is not entirely analogous to the civil case of *Zubulake v. UBS Warburg*

Service Providers Can: Preserving Privacy in Email Contents, 16 VA. J. L. & TECH. 253, 257 (2011).

[164] *See* David Degnan, *Accounting for the Costs of Electronic Discovery*, 12 MINN. J. L. SCI. & TECH. 151, 151 (2011).

("*Zubulake IV*").[165] In *Zubulake IV*, the majority of the $273,649 production costs stemmed from restoring five offline magnetic tapes and attorney fees.[166] Data stored in the cloud is clearly online and available for access. But the physical act of locating and copying the data may still take considerable time. For example, Amazon offers an export service, which copies and mails customers' data in a storage device.[167] This service costs $80 per storage device handled plus $2.49 per data-loading hour.[168] These costs are unlikely to approach the costs of magnetic tape restoration, but the costs to *analyze* large data volumes will likely dwarf the data production costs.[169] Importantly, an IaaS cloud provider may be unable to search the corpus of data and produce specific evidence (e.g., a particular file), but rather would have to hand over the whole data set.[170]

IV. RESPONSIVE STRATEGIES

[44] Part II discussed the logistics and pitfalls of obtaining cloud data. This section describes defenses and responses that could discredit that evidence. Some issues parallel the scrutiny of any evidence, including the *Daubert* or *Frye* tests.[171] Other issues arise explicitly from the use of cloud technology, such as environment complexity and jury comprehension.

---

[165] 216 F.R.D. 280 (S.D.N.Y. 2003).

[166] *Id.* at 289-90.

[167] *AWS Import/Export*, AMAZON WEB SERVICES, http://aws.amazon.com/importexport/ (last visited Sept. 4, 2012).

[168] *Id.*

[169] If a cloud customer arbitrarily had two terabytes of data in the cloud, it would take nearly 10 hours to copy to a USB hard drive, totaling $104.90. *Id.* One article estimates forensic analysis averaging $1000 per gigabyte, bringing two terabytes to $2 million. *See* Degnan, *supra* note 164, at 162.

[170] *See* David Colarusso, Note, *Heads in the Cloud, A Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, 17 B.U. J. SCI. & TECH. L. 69, 91 (2011).

[171] *See generally* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993); Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

[45] It is worth noting that the law deals in imperfect analogies.[172] This makes explaining the relation between the cloud and the law difficult for all involved. Despite cursory similarities between searching a cloud-based file system and a physical filing cabinet, the injustice served by that analogy should raise doubt about its applicability.

[46] By their nature, cloud-computing environments are more complex than a single computer or a server.[173] Cloud environments have many layers of implementation that must be trusted to produce authentic data.[174] In 2009, for example, researchers demonstrated a working exploit to break out of a virtual machine and attack the host.[175] In a real-word situation, this could have destroyed confidence in the forensic evidence. Courts have repeatedly ruled that merely showing that an action is *possible* does not prove that it is so.[176] Nevertheless, computer malfunction and

[172] *See* Serena Mayeri, *Reconstructing the Race-Sex Analogy*, 49 WM. & MARY L. REV. 1789, 1837-38 (2008) (discussing the Race-Sex analogy in *Regents of University of California v. Bakke*, 438 U.S. 265 (1978)).

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

[174] *See supra* Part II.A.

[175] *See* Video Demonstrating Cloudburst Module, IMMUNITY INC., http://www.immunityinc.com/documentation/cloudburst-vista.html (last visited Aug. 19, 2012).

[176] *See, e.g.*, Noblesville Casting Div. of TRW, Inc. v. Prince, 438 N.E.2d 722, 731 (Ind. 1982) (mere possibilities will not suffice to place a fact in issue; "[o]f course, an expert's opinion that something is 'possible' or 'could have been' may be sufficient to sustain a verdict or award when it has been rendered in conjunction with other evidence concerning the material factual question to be proved"). The "what if" scenarios for data tampering in the cloud are numerous, a non-comprehensive list of which includes: (1) data could be tampered with in transit over the network; (2) redundant copies of the data could have gotten out of sync; (3) the data owner's credentials could have been compromised, resulting in false data creation or data tampering; (4) there are opportunities for many insider threats at the provider; (5) the hypervisor may be insecure allowing a malicious user to manipulate other virtual machines; (6) the host operating system could be insecure; or (7) there could be weak or no encryption on the provider's internal infrastructure for data in transit or data at rest.

malfeasance must be investigated and can cause fact-finders to question the evidence. The hypervisor is especially vulnerable to scrutiny given its powerful position to see and manipulate all virtual machines that it controls, including concomitant data.[177] Many cloud service providers use custom proprietary hypervisors that the global security community has neither seen nor independently audited.[178]

[47] This evidentiary complexity can challenge judges and juries who lack knowledge about cloud computing. Such complex evidentiary analysis might leave the lay juror "spinning with information too strange to digest and often too intimidating to ponder."[179] Much has been written, particularly over the last twenty years, about how juries comprehend complex evidence, including highly scientific evidence such as DNA.[180]

---

[177] *See* Jansen & Grance, *supra* note 102, at 2 (noting that a hypervisor "is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines and is common to IaaS clouds" and "supports other application programming interfaces to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances," which is vulnerable to compromise because it "causes an increase in the attack surface" via the "additional methods (e.g., application programming interfaces), channels (e.g., sockets), and data items (e.g., input strings) an attacker can use to cause damage to the system").

[178] *See, e.g.*, Clive Longbottom, *Will Hypervisors need a Supravisor?*, VNUNET, 1-2 (2008), *available at* http://www.quocirca.com/media/articles/042008/220/Will%20Hypervisors%20need%20a%20Supravisor.pdf.

[179] Keith E. Broyles, *Taking the Courtroom into the Classroom: A Proposal for Educating the Lay Juror in Complex Litigation Cases*, 64 GEO. WASH. L. REV. 714, 714 (1996); *see also* DONALD E. SHELTON, FORENSIC SCIENCE IN COURT: CHALLENGES IN THE TWENTY FIRST CENTURY 117 (Gregg Barak ed. 2010).

[180] *See, e.g.,* Joe S. Cecil et al., *Citizen Comprehension of Difficult Issues: Lessons from Civil Jury Trials*, 40 AM. U. L. REV. 727, 728-29 (1991) (citing J. JOSEPH F. WEIS, JR. ET AL., FED. COURTS STUDY COMM., REPORT OF THE FEDERAL COURTS STUDY COMMITTEE 97 (1990), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/repfcsc.pdf/$file/repfcsc.pdf (recommending comprehensive examination of how courts handle scientific and technological complexity in litigation)).

Jurors have almost certainly used the Internet,[181] but this says nothing about their comprehension of how it or their computer works. Cloud computing is one of today's most complex computing environments and it is likely to challenge even the most technically inclined juror. As such, evidence and expert witness testimony must be presented artfully.

[48] Cloud providers currently execute search warrants and subpoenas for law enforcement and litigants.[182] In this regard, cloud providers act no differently than any other Internet-based entity. But doing so may raise a conflict of interest.[183] Cloud providers are interested in protecting their reputations, so they are not likely disinterested.[184] Furthermore, the provider may have neither the discernment nor the authority to determine what other evidence is relevant, responsive, or in plain view.[185] Lastly, in

[181] *See Internet Adoption*, PEW INTERNET & AM. LIFE PROJECT (2012), http://www.pewinternet.org/Static-Pages/Trend-Data-(Adults)/Internet-Adoption.aspx (noting that, as of April 2012, 82% of American adults use the Internet).

[182] *See supra* Part III.B.

[183] *See, e.g.*, David D. Cross & Emily Kuwahara, *E-Discovery and Cloud Computing: Control of ESI in the Cloud*, 1 EDDE J., no. 2, Spring 2010 at 3, *available at* http://www.crowell.com/documents/e-discovery-and-cloud-computing-control-of-esi-in-the-cloud.pdf (noting that "[w]ith a third-party in possession of data that parties to litigation may view as their own (or a court may view as belonging to them), issues surrounding the duties to preserve and produce become more pronounced."); *see also* Gruenspecht, *supra* note 14, at 545, 551 (noting that cloud service providers have a "lack of interest in disputing governmental requests," but that, for document creators, "[t]he privacy problem presented is clear: searching [electronic storage] in a comprehensive way can expose both crimes and embarrassing private information that can be admissible in court under the plain view exception") (internal quotation marks omitted).

[184] *See* ACHIEVING DATA PRIVACY IN THE CLOUD, PONEMON INSTITUTE LLC 3 (June 2012), *available at* http://download.microsoft.com/download/F/7/6/F76BCFD7-2E42-4BFB-BD20-A6A1F889435C/Microsoft_Ponemon_Cloud_Privacy_Study_US.pdf. *But see* Gruenspecht, *supra* note 14, at 550-51 ("A third-party subpoena recipient rarely disputes the request, or even the delay of notice. The problems with subpoenas to cloud computing data service providers go beyond the service providers' lack of interest in disputing governmental requests.").

[185] *See* Gruenspecht, *supra* note 14, at 551 ("[C]loud computing data holders, unlike traditional business records holders, may not be in a position to address the questions of

civil matters, providers lack the incentive to do thorough and accurate searches, particularly because such searches can be expensive.[186] Because the requesting parties often lack technical knowledge of the cloud providers' systems—and are often physically remote from the providers who execute the searches—those parties' oversight over those searches is often limited or nonexistent.[187] Rigorous guidelines, such as how to challenge the scope and procedure of the search, are currently lacking or absent. Barring these changes, it would be preferable for an independent third party to execute the warrant or subpoena upon a cloud provider.[188] Until the process of how a provider executes a search is well understood, however, the requesting party would be wise to call the technicians to testify about their methodology.[189] As already noted, a party "need not

relevance and particularity, since they do not know what information they possess. Even a data holder willing to dispute a subpoena may not have sufficient knowledge to argue against its unreasonableness."). Courts disagree about what constitutes "plain view" in digital evidence. *Compare* United States v. Williams, 592 F.3d 511, 521-22 (4th Cir. 2010) (holding that evidence viewable on a computer or electronic media may be seized under the plain view exception)*, with* United States v. Mann, 592 F.3d 779, 782, 785-86 (7th Cir. 2010) (holding that evidence uncovered while searching a computer pursuant to a warrant falls within the plain view exception).

[186] *See* FED. R. CIV. P. 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.").

[187] *See* Cross & Kuwahara, *supra* note 183, at 1 (noting that "cloud computing may dramatically expand the number of places that ESI may reside—and may significantly increase the complexity and difficulty of locating and obtaining that data"). *But cf.* FED. R. CIV. P. 26(f); Shira A. Scheindlin & Jonathan M. Redgrave, *Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure*, 30 CARDOZO L. REV. 347, 356 (2008) (noting a Rule 26(f) conference requires that "parties must be prepared to disclose information about their computer systems, including where and for how long information is maintained").

[188] *See* Jerry Archer et al., *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, CLOUD SECURITY ALLIANCE, 42-43 (2011), https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (noting that a cloud service provider "might be tempted to reply" to a request for client data by providing a broad range of data to the requestor without questioning the validity of the request).

[189] *See* FED. R. EVID. 702.

call each of the technicians who did the search so long as it presents a witness who 'can explain and be cross-examined concerning the manner in which the records are made and kept.'"[190]

[49] The cloud's nebulous nature makes evidentiary admission difficult. The *Daubert*[191] and *Frye*[192] standards measure the scientific validity and relevance of forensic evidence. The *Daubert* factors include determining whether a theory or technique has been tested, whether it has been subject to peer review and publication where there is a known error rate, and whether the theory or technique is generally accepted within the relevant scientific community.[193] Similarly, the *Frye* standard requires that the method "be sufficiently established to have gained general acceptance in the particular field."[194] The Supreme Court in *Daubert* held that Federal Rule of Evidence 702 superseded *Frye* as the applicable standard for admitting expert scientific evidence in federal courts,[195] but some state courts still follow the "general acceptance" standard articulated in *Frye*.[196]

[50] Because cloud forensics is a relatively new discipline, establishing

[190] United States v. Cameron, 733 F. Supp. 2d 182, 188 (D. Me. 2010) (citing Wallace Motor Sales, Inc. v. Am. Motors Sales Corp., 780 F.2d 1049, 1061 (1st Cir. 1985)).

[191] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 589 (1993) (holding that although scientific evidence does not have to be generally accepted, any evidence admitted must be both relevant and reliable).

[192] Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923) (finding that experts should be permitted to testify only about scientific principles that are generally accepted in their fields).

[193] *Daubert,* 509 U.S. at 593-94.

[194] *Frye*, 293 F. at 1014.

[195] *Daubert,* 509 U.S. at 589 n.6 ("[W]e hold that *Frye* has been superseded.").

[196] *See, e.g.*, State v. Sercey, 825 So.2d 959, 978 (Fla. Dist. Ct. App. 2002) ("Notwithstanding the U.S. Supreme Court's ruling in *Daubert* that the Federal Evidence Code had superceded [sic] the *Frye* test in federal court proceedings, Florida has continued to adhere to *Frye*.").

all of these factors is difficult.[197] Courts have held that popular forensic tools like EnCase have passed the *Daubert* test in part because of their commercial availability, testing by the government,[198] long-term use, and extensive scientific acceptance.[199] But in the forensic community, techniques for remote forensics, let alone cloud forensics, rarely enjoy any consensus.[200] Forensic practitioners who are unfamiliar with cloud environments are often tempted to use their existing tools like EnCase.[201] Even the advertised features of commercial tools such as EnCase, which can be used for remote forensics, have not been tested for accuracy or error rate, nor have they been tested in court.[202] This software is not unassailable. In 2007, experts analyzed the authentication between the remote EnCase client and the server, allegedly finding vulnerability that could purportedly allow an attacker to corrupt or falsify data.[203]

---

[197] *See* Archer et al., *supra* note 188, at 42 (noting that questions regarding authentication, admissibility, and credibility are not easily resolved by establishing that the information was stored in the cloud).

[198] The National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) project is charged with testing, measuring the effectiveness of, and certifying digital forensic tools. NIST evaluated EnCase 6.5 in September 2009, but has never evaluated EnCase Enterprise, which includes the remote forensic features. *See CFTT Project Overview*, NAT'L INST. OF STANDARDS AND TECH. (Aug. 20, 2003), http://www.cftt.nist.gov/project_overview.htm.

[199] *See* GUIDANCE SOFTWARE, *supra* note 2, at 55-66 (summarizing trial and appellate court decisions addressing the admissibility of EnCase software).

[200] *Id.* at 1.

[201] JOSIAH DYKSTRA & ALAN T. SHERMAN, CYBER DEFENSE LAB, DEPARTMENT OF CSEE, ACQUIRING FORENSIC EVIDENCE FROM INFRASTRUCTURE-AS-A-SERVICE CLOUD COMPUTING: EXPLORING AND EVALUATING TOOLS, TRUST, AND TECHNIQUES 7-8 (Apr. 18, 2012), http://publications.csee.umbc.edu/publications/560 (follow "DFRWS_Dykstra.pdf" hyperlink).

[202] *See* Archer et al., *supra* note 188, at 97 (explaining that until accepted best practice guidelines are developed, it is unclear whether the analysis results for cloud will stand up in court).

[203] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Vulnerability Note VU912593: Guidance EnCase Enterprise uses weak authentication to identify target machines*, U.S.

[51] As one district court noted, "[i]t is the rare case that a litigant does not allege some deficiency in the production of electronically stored information." [204] Producing cloud-based evidence is no different, particularly since that kind of evidence will likely remain novel for years to come.

[52] Many issues can be raised about the deficiency of production of cloud-based ESI. Such questions may include:

> (1) Who from the provider executed the search warrant, what were their credentials, and how was the search conducted?
>
> (2) Can the technician who executed the search attest to the data's reliability and authenticity, including:
>
> (a) the security of the workstation used to execute the search,
>
> (b) the security of the network to prevent data tampering over the network, and
>
> (c) a record of who had access to the data?
>
> (3) Does the provider maintain aggressively enforced records management policies that can provide authenticity and authentication of the data, perhaps in the form of data provenance?
>
> (4) Can the provider attest to the reputation and integrity of the cloud infrastructure, including the hypervisor and host operating system?

DEP'T OF HOMELAND SECURITY (Nov. 9, 2007), http://www.kb.cert.org/vuls/id/912593 (last updated Nov. 20, 2007).

[204] Covad Commc'ns. Co. v. Revonet, Inc., 258 F.R.D. 5, 13 (D.D.C. 2009).

> (5) Is it possible that important evidentiary data once existed and has been deleted, and if so, is there any record of it?

As these questions illustrate, the most vulnerable aspects of cloud discovery are expert-witness testimony and the forensic methodology used.[205]

[53] Finally, cases addressing cloud-based evidence are unlikely to produce much definitive judicial guidance because the technology is relatively novel.[206] Cloud computing technology has evolved over time and continues to change regularly.[207] Adjudicating too narrowly on cloud-specific issues would be premature even though courts can, and do, broadly apply certain established principles (e.g., civil and criminal rules of evidence, Fourth Amendment search and seizure).[208] In fact, Justice Sotomayor's recent concurring opinion discusses potentially changing attitudes about the expectation of privacy in data given to third parties in the digital age: "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[209]

---

[205] *See* Cross & Kuwahara, *supra* note 183, at 5.

[206] *See* Christine Soares, *Applying E-Discovery Best Practices to Cloud Computing*, LAW.COM, (Feb. 10, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202541881944.

[207] Amazon Web Services has announced new features or service changes at least one time per month during 2011 and 2012. *Amazon Web Services Releases*, AMAZON, http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsWebservices (last visited Sept. 5, 2012). Other providers have a similar pace of change.

[208] *See* Matthew A. Verga, *Cloudburst: What Does Cloud Computing Mean to Lawyers?*, 5 J. LEGAL TECH. RISK MGMT. 41, 48-49 (2010) (discussing the application of the Federal Rules of Civil Procedure to cases involving cloud computing).

[209] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.") (internal citations omitted).

V. CONCLUSION

[54] Cloud computing is a tremendous advancement in the history of computation, due in large part to technological convergence.[210] The economics of the paradigm will drive companies and individuals to increase growth and adoption rates. Where the people, the data, and the money go, so follows crime and litigation.[211] While investigators and litigators struggle with the emerging problems of acquiring and analyzing cloud data, the law must prepare for evidentiary challenges associated with acquiring and presenting cloud data. The first public cases involving cloud-based ESI are emerging and those involved in those cases have a rare opportunity to develop electronic discovery.[212]

[55] The issues presented here are not wholly unique to cloud computing and we stress that these issues can also be raised regarding other Internet-derived data, such as social networks and web-based e-mail. Some important choices must be made to improve the approach to online data. We have proposed three new ideas. First, online users should have a reasonable expectation of their online data's geographic location.[213] Second, cloud providers should not be permitted to execute search warrants or subpoenas without the introduction of more rigorous operating guidelines.[214] Third, remote forensics should be permitted from anywhere, guided by the laws of the provider's forum.[215] If implemented, these changes will likely provide a stronger foundation to gathering and

[210] *See* Araiza, *supra* note 39, at 7-8; Couillard, *supra* note 50, at 2216.

[211] *See* Archer et al., *supra* note 188, at 35; J. Mark Ramseyer, *Litigation and Social Capital: Divorces and Traffic Accidents in Japan*, *in* THE HARVARD JOHN M. OLIN CENTER FACULTY DISCUSSION PAPER SERIES, No. 727, at 6 (2012), *available at* http://www.law.harvard.edu/programs/olin_center/papers/pdf/Ramseyer_727.pdf.

[212] *See* Verga, *supra* note 208.

[213] See *supra* Part III.A.

[214] See *supra* Part III.B.

[215] See *supra* Part IV.

analyzing cloud-computing evidence in ways that are more robust and defensible.