NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
11 N.C. J.L. & TECH. ON. 115(2009)

SPRING TRAINING FOR ELECTRONIC SEARCH: EXAMINING *U.S. V. COMPREHENSIVE DRUG TESTING, INC.* WITH REGARDS TO EVOLVING TRENDS IN COMPUTING

John T. Kivus[1]

This Recent Development discusses the framework for electronic search that was laid out by the Ninth Circuit in U.S. v. Comprehensive Drug Testing, Inc. *Though the Ninth Circuit's framework has positive elements, the framework is fatally flawed because it does not account for the rapid evolution of computing technologies and does not account for recent computing trends, such as cloud computing. This Recent Development makes recommendations about how the existing parts of the Ninth Circuit's framework could be modified to create an electronic search framework that would provide lasting privacy protections to individuals in a world of rapid technological evolution.*

I. WARM-UPS: INTRODUCTION

The Ninth Circuit's recent decision in *U.S. v. Comprehensive Drug Testing, Inc.*[2] set forth a new framework for handling the search of electronic data.[3] The framework attempted to provide generic guidelines to those executing searches for specific, electronically stored data in a much larger set of electronic data.[4] Its main element was separating those who do the initial data evaluation from those who will ultimately be prosecuting the

[1] J.D. Candidate, University of North Carolina School of Law, 2011. I wish to give a special thank you to my family, especially my parents, who have given me support and encouragement in the face of any and all obstacles.

[2] U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378 (9th Cir. Aug. 25, 2009).

[3] *Id.*

[4] *See generally* Comprehensive Drug Testing, Inc., 2009 WL 2605378 (creating a new framework for the execution of warrants that deal with electronic data).

crime.[5] The Ninth Circuit's usage of the "container approach"[6] in its framework and the fact that the court did not succumb to any rudimentary electronic data search fallacies[7] show that it has a fairly solid understanding of computing and electronic data storage. Despite this understanding, however, there are fundamental problems with the framework[8] that make it unable to last as a long-term standard for those conducting electronic searches. This Recent Development will explore those problems and, more importantly, how the framework does not handle rapid developments in the changing computing landscape, especially with the expansion of "cloud computing"[9] services. Additionally, this Recent Development will make recommendations for how the Ninth Circuit's framework could be modified to account for off-site cloud computing services when executing search warrants.[10] It will also recommend that companies who run large cloud computing data stores should be given the opportunity to assist in the execution of search warrants by performing some data extraction themselves.[11] These recommendations would create a

---

[5] *Id.*

[6] Thomas K. Clancy, *Symposium: The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 209 (2005). Much like a file cabinet that stores individual files, and is a container for those files, a computer is a container for the files it stores. Additionally, the container for the files might be defined at a smaller level than the computer itself, perhaps the particular disk that files are stored on or even a particular directory on a disk. *Id.* at 196.

[7] *Id.*

[8] *See* discussion *infra* Part II.E.

[9] Cloud computing refers to the storage of information on servers that are accessed via the Internet. Frequently these servers are not owned by the individual accessing them but are instead maintained by a third party who specializes in server maintenance and upkeep. Eric Knorr & Galen Gruman, What Cloud Computing Really Means, INFOWORLD, (April 7, 2008), http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology).

[10] *See* discussion *infra* Part.II.E.6.

[11] *Id.*

framework that would hold up in a world of rapid technological expansion.

In order to provide foundation for this discussion, this Recent Development will provide a brief overview of the facts in *Comprehensive Drug Testing* and a brief look at the reasoning for the establishment of the electronic search framework in that same decision in Part II.A. In Part II.B, this Recent Development looks at general issues found in electronic search (Part II.B.1), and also examines a previous attempt to establish an electronic search framework (Part.II.B.2). Part II.C lays out the framework the Ninth Circuit established. The analysis of the positive elements of the framework and the negative elements of the framework follow in parts II.D and II.E, respectively. In addition to the analysis of the framework in Parts II.E.1 through Parts II.E.4, Part II.E.5 discusses whether a search warrant is required in a cloud computing situation. Parts II.E.6 and II.E.7 lay out a framework that the legislature could implement to provide the flexibility required to handle electronic search in the future.

II. GAME TIME: ANALYSIS

A. *Starting Lineups: Facts and Holding*

In 2002, the federal government executed a search warrant for ten players the government had probable cause to suspect had tested positive for "performance enhancing drugs"[12] during Major League Baseball's ("MLB") initial drug testing program.[13] Though

---

[12] Performance enhancing drugs is a general term for substances taken to improve the quality of someone's athletic play. Craig Freudenrich, HowStuffWorks: Performance Enhancing Drugs, http://www.howstuffworks.com/athletic-drug-test.htm (last visited Sept. 25, 2009) (on file with the North Carolina Journal of Law & Technology). The category of substance most commonly referred to by the term performance enhancing drug is steroids, however, the term can also refer to stimulants that are used to raise the alertness of players. *Id.*

[13] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378, at *1; Drug Policy coverage: MLB.com News, http://mlab.mlb.com/mlb/news/drug_policy.jsp?

the warrant listed the ten baseball players for which the government could seize test results, the "government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball."[14]

The Ninth Circuit began its analysis of the government's search protocol with an application of *U.S. v. Tamura*,[15] explaining how the government should have performed an initial review[16] of the data by "computer personnel"[17] before investigators received access to the data. The court then explained how the government violated this procedure by using all the information that was taken for the initial review.[18] In response to the government's actions, the Ninth Circuit established a framework that should be used during the execution of search warrants concerning electronic evidence going forward.[19]

B. *Reviewing the Scouting Reports: General Electronic Search and Previous Decisions*

1. *Batting Averages: General Trends in Electronic Search*

Before reviewing the framework for electronic search set out by the Ninth Circuit in *Comprehensive Drug Testing,* it is helpful to both review some of the issues that are present when executing a search warrant on electronic evidence and to review the previous

---

content=timeline (last visited Sept. 25, 2009) (on file with the North Carolina Journal of Law & Technology).

[14] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378, at *1.

[15] *See generally* U.S. v. Tamura, 694 F.2d 591 (Ninth Cir. 1982) (holding that when document searches require data analysts to move data offsite, the government must indicate in the warrant the necessity to move the data offsite or have the warrant amended to reflect the necessity to move the data offsite. Additionally, the government may only use those documents for which the warrant said the government had probable cause to seize even if the government was allowed to remove more documents during its initial search).

[16] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378, at *7.

[17] Computer personnel are law enforcement personnel trained in searching and seizing computer data. *Id.* at *4.

[18] *Id.* at *9

[19] *See* discussion *infra* Part II.C.

framework the Ninth Circuit set forth for electronic search. There are two sets of problems that have to be dealt with when performing an electronic search: 1) problems associated with searching for data electronically and 2) problems associated with finding the specific data authorized by the warrant within a much larger amount of electronic data. Looking first at the nature of electronic searches themselves, one issue that arises is that searching computer files entails complications that are not common when searching through physical evidence. There are many ways that a suspect could mislead authorities by disguising files in either file name or file extension.[20] Another problem is trying to open particular files and particular file types. A number of files require a specific program or type of program to open them,[21] and an analyst cannot be expected to have every program for each individual file type at his disposal.[22] Beyond simply opening the files with a particular program, the files could also be encrypted.[23] Encryption types can vary from simply requiring a

---

[20] *Id.* at *3. In order to mislead investigators about the contents of a file, suspect could change the name of a file regarding bomb instructions from "bomb.instructions" to "puppy.pictures." Additionally, he or she could change the files extension so that a document has a file extension normally associated with an image (i.e. rename all .txt files to .jpg).

[21] Certain Document files (.docx files) require Microsoft Word or one of Microsoft's conversion tools to open. Introducing the Office (2007) Open XML File Formats, http://msdn.microsoft.com/en-us/library/aa338205.aspx (last visited Oct. 22, 2009) (on file with the North Carolina Journal of Law & Technology). Some image files, such as .psd files require either Adobe Photoshop, PSD File Format, http://www.graphicsacademy.com/format_psd.php (last visited Oct. 22, 2009) (on file with the North Carolina Journal of Law & Technology), or a third party program that has built in PSD support. *See e.g.* Pixelmator: an Amazing Tool for an Amazing Price | Fuel Your Interface, http://www.fuelyourinterface.com/pixelmator-an-amazing-tool-for-an-amazing-price/ (last visited Oct. 22, 2009) (on file with the North Carolina Journal of Law & Technology).

[22] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378 at *3.

[23] Encryption is "the process of encoding information in such a way that only the person (or computer) with the key can decode it." Jeff Tyson, HowStuffWorks: How Encryption Works, http://computer.howstuffworks.com/encryption.htm (last visited Oct. 23, 2009) (on file with the North Carolina

password to requiring thumbprint scanning[24] to even using a computer's built-in camera to perform facial recognition before allowing access to the files.[25] This is in addition to corporate security methods that might include the use of a key installed on a universal serial bus ("USB") drive[26] that has to be connected to the device or even a time sensitive token that changes every few seconds and must be entered.[27] Further exacerbating the encryption problem is the potential hazard that if the correct data access procedures are not followed, the data will be compromised.[28]

The second set of problems deals with figuring out exactly what type of data the warrant covers. For example, if the warrant is for pornographic images of a child, does that mean the computer analyst can only look at files that have extensions commonly associated with images or can the analyst also look at files that have extensions commonly associated with documents? As evidenced by the preceding question, the issues of electronic search and the more general issues of searching for specific information within the context of a warrant can be tightly

---

Journal of Law & Technology).

[24] Jessie Seyfer, Fingerprint Security Gets Handier, http://www.wired.com/science/discoveries/news/2000/10/39726 (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology).

[25] John Leyden, Laptop Facial Recognition defeated by Photoshop, http://www.theregister.co.uk/2009/02/19/facial_recognition_fail (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology).

[26] Varun Kashyap, Use your USB stick as a key to boot your PC, http://www.makeuseof.com/tag/prevent-pc-from-booting-if-your-usb-drive-is-not-inserted (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology).

[27] RSA SecurID, http://www.rsa.com/node.aspx?id=1156 (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology).

[28] Data can be booby trapped so that when not accessed in the manner configured by the user, the data automatically corrupts itself or deletes itself. Samiya Anwar, Cyber crime increases need for computer forensics—Instablogs, http://samiyaanwar.instablogs.com/entry/cyber-crime-increases-need-for-computer-forensics/ (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

intertwined. The Ninth Circuit had to take these types of issues into account when developing its electronic search framework.[29]

2. *Previous at Bat: Prior Decisions Involving Electronic Search*

The Ninth Circuit's first attempt to apply the standards of *U.S. v. Tamura*[30] to a case involving electronic evidence was in *U.S. v. Hill.*[31] In order to work around the problems of file name and file extension discussed previously,[32] the court set up a system where the government could apply to a magistrate for permission to make a "wholesale seizure,"[33] if that type of seizure is reasonable in a given case.[34] This particular framework received criticism, however, as it essentially allowed the police to open any file on a computer while conducting a search.[35]

C. *Starting Pitchers: The Ninth Circuit Electronic Search Framework*

The parts of the electronic search framework set forth by the Ninth Circuit that are relevant[36] to this Recent Development are as

---

[29] *See generally* Comprehensive Drug Testing, Inc., 2009 WL 2605378 (creating a new framework for executing electronic search based on a search warrant).

[30] *See generally* U.S. v. Tamura, 694 F.2d 591 (9th Cir. 1982).

[31] 459 F.3d 966 (10th Cir. 2006).

[32] *See* discussion, *supra* note 20.

[33] *Hill,* 459 F3d at 975.

[34] *See generally Hill*, 459 F.3d 966 (holding that if the government can demonstrate a reasonable need then they can make a wholesale seizure of electronic search information that can than later be sorted through for information that falls within the confines of the warrant).

[35] For a full examination of the standards in U.S. v. Hill, 459 F.3d 966 (10th Cir. 2006) refer to G. Robert McClain, Jr., *United States v. Hill: A New Rule, But No Clarity For the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071 (2007) (examining the standards set forth in U.S. v. Hill in regards to electronic search).

[36] In addition to those standards listed, there is also the requirement that the "government waive reliance on the plain view doctrine" *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378, at *18. Though the reliance on the plain view doctrine has implications for electronic search generally, its ramifications are

follows: (1) the initial search and separation of the data has to be performed by either computer personnel or some other third party,[37] (2) any prior attempts to seize the information and whether or not there is a chance the information will be destroyed has to be disclosed,[38] (3) the searches should be created in such a way that the computer personnel find only information for which there is probable cause and give only that information over to the case agents,[39] and (4) any seized evidence that does not fit within the confines of the warrant must be returned or destroyed.[40] The Ninth Circuit viewed this framework as a way to balance the need to examine[41] files to view their contents with the need to insure that every search warrant dealing with electronic evidence does not result in blanket warrant to seize all electronic information.[42]

D. *Hitting Singles, Doubles and Triples: Positive Elements of the Ninth Circuit's Framework*

One of the weaknesses of the Ninth Circuit's framework is that it, as a whole, will be unable to adapt to changing computing trends and will be unable to endure rapid technological development. There are some approaches, however, that should adapt to changing computing trends and should endure such technological development. The most important of these items is the adoption of what Professor Thomas Clancy[43] would refer to as

---

beyond the scope of this Recent Development. For discussion of the impact of the *Comprehensive Drug Testing, Inc.* decision with reference to the plain view doctrine, see Jeremy D. Frey, *Ninth Circuit Decision has Major Implications for Search Warrants Authorizing Seizure of Computer Information*, E-COMMERCE L. REP., Sept. 2009, at 11.

[37] *Comprehensive Drug Testing, Inc*., 2009 WL 2605378, at *18

[38] *Id.* at *16.

[39] *Id.*

[40] *Id.*

[41] Files can be examined by "opening it and looking, using specialized forensic software, keyword searching or some other such technique" *Id.*

[42] *Id.* at *6.

[43] Thomas Clancy created the University of Mississippi's Cyber Crime Initiative to assist in the training of the government agents for computer crime

the "container"[44] approach to a computer search.[45] Utilizing this model makes the court's application of *Tamura*[46] much more appropriate and also allows for future expansion of this framework as more types of data "containers" arise.[47] Essentially, Professor Clancy maintains that computers themselves are "containers and the data [these containers] contain are mere forms of documents".[48] This abstraction allows for various forms of computing storage (both internal and external) to fall within the scope of the warrant when searching for particular information.[49]

The Ninth Circuit's framework follows the idea that the warrant "may be as extensive as reasonably required to locate the items described in the warrant."[50] This includes making no restrictions about the file types or extensions when creating the search standards.[51] This kind of flexibility allows warrants to easily handle situations where a new file extension for even the same type of file is released.[52] Additionally, the Ninth Circuit

---

investigations. Profile of Thomas Clancy, http://www.law.olemiss.edu/faculty/clancy_thomas.html (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

[44] CLANCY, *supra* note 6, at 263.

[45] *Id.*

[46] U.S. v. Tamura, 694 F.2d 591 (9th Cir. 1982).

[47] For further examples of how to define "containers" in regard to electronic search see the discussion, *infra* Part II.E.6, defining what the container size should be for off-site cloud computing data stores.

[48] CLANCY, *supra* note 6, at 195.

[49] There are still some issues with this abstraction, especially when it turns to issues involving cloud computing. *See* discussion *infra* Part II.E.3.

[50] U.S. v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006) (quoting United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982)).

[51] CLANCY, *supra* note 6, at 209.

[52] Recently, the Microsoft Word document format, one of the most prominent file formats, was upgraded to a new Open XML format (Microsoft Word Docx Page). If the Ninth Circuit's framework required warrants to list out specific file extensions, then a warrant for Microsoft Word files that were saved in .doc format would not cover Microsoft Word files that were saved in .docx format.

wisely did not make any declarations that would affect data stored along with the file, commonly called "metadata."[53]

E. *Strike Outs: Negative Elements of the Ninth Circuit's Framework*

The Ninth Circuit's framework raises both general issues and specific issues. The general issues arise from the nature of electronic search and indicate that any framework around electronic search would not be sustainable long term.[54] The specific issues arise from this particular framework's failure to account for recent computing trends and indicate that this framework will not hold up against trends such as "cloud computing."[55]

---

[53] Metadata can include something as basic as the author of the document, but also may include items such as the revision history of a particular file. For a helpful primer on metadata, *see* Chris Taylor, An Introduction to Metadata (July 29, 2003) http://www.library.uq.edu.au/iad/ctmeta4.html (last visited Sept. 25, 2009) (on file with the North Carolina Journal of Law & Technology). One example of how metadata can affect a lawsuit occurred in 2004 in a series of lawsuits known as the "SCO Lawsuits." ROBERT JONES, INTERNET FORENSICS 138 (O'Reilly Media, 2006). During document discovery it was discovered that the editing history (i.e. a type of metadata) of the initial lawsuit filing revealed legal strategy that was going to be used in the trial. *Id.* Apparently this strategy information was originally in the lawsuit filing document but deleted before the document was formally filed. *Id.* A quick examination of the metadata, however, revealed this information to the opposing party and gave said party the advantage of knowing what the filer of the lawsuit intended to use for his legal strategy. *Id.* Since the Ninth Circuit did not make any declarations about metadata in their framework, it leaves the door open for computer personnel to find incriminating evidence on criminals attempting to cover their tracks. For example, a person who deleted a recipe for a bomb from a document with other recipes of food items could leave a metadata trail that allows computer personnel to find the original bomb recipe.

[54] *See* discussion *infra* Parts II.E.1, II.E.2.

[55] *See* discussion *infra* Part.II.E.3. *See also* KNOOR & GRUMAN, *supra* note 10.

1. *Old Reliable: General Issues with the Ninth Circuit Framework*

The general issues arise mostly from the rapid speed at which technology evolves.[56] Even the operating system, one of the bedrocks of any computer's function, and facilitator of many of the basic operations that are necessary for a computer to function, has gone through multiple evolutionary cycles recently.[57]

[56] One of the most widely cited illustrations of the speed of technological evolution is Moore's Law, which states that "the number of transistor's on a chip will double every two years." *See* short explanation of Moore's Law, http://www.intel.com/technology/mooreslaw (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology). For further examples of the speed of computer evolution *see infra* Part II.E.2.

[57] *See* Curt Franklin & Dave Coustan, *How Operating Systems Work*, http://computer.howstuffworks.com/operating-system.htm (explaining how operating systems function) (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology). To illustrate the rapid cycle of operating system evolution, survey the amount of operation system releases since the release of a text on electronic search in 2004. *See* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME, (Academic Press, 2004) (2000). Since this text was published, two new versions of the Microsoft Windows operating system have been released, Windows 7 and Vista. *See* Windows 7—Home, http://windows.microsoft.com/en-US/windows7/products/home (last visited Sept. 12, 2009) (showing the release date for Windows 7, the latest version of Microsoft Windows) (on file with the North Carolina Journal of Law & Technology); Vista Gets Official Release Dates, http://apcmag.com /vista_gets_official_release_dates.htm (last visited Sept. 12, 2009) (showing the release date for Windows Vista, the second latest version of Microsoft Windows) (on file with the North Carolina Journal of Law & Technology). Three major versions of the Mac OS X operating system have also been released. *See* Apple Announces Mac OS X 10.4 "Tiger" Release Date, http://www.osnews.com/story/10268 (last visited Sept. 12, 2009) (showing the release date of OS X 10.4 "Tiger" the third most recent version of Mac OS X) (on file with the North Carolina Journal of Law & Technology); Mac OS X 10.5 (Leopard) Release Date in 10 Days!, http://cybernetnews.com/mac-os-x-105-leopard-release-date-in-10-days/ (last visited Sept. 12, 2009) (showing the release of Mac OS X 10.5 "Leopard", the second most recent release of Mac OS X) (on file with the North Carolina Journal of Law & Technology); Apple to Ship Mac OS X Snow Leopard on August 28, http://www.apple. com/pr/library/2009/08/24macosx.html (last visited Sept. 12, 2009) (showing the release of Mac OS X 10.6 "Snow Leopard", the most recent release of Mac OS X) (on file with the North Carolina Journal of Law and Technology). Linux

Additionally, the types of services that individuals use on platforms like the Internet are changing rapidly. For example, Eoghan Casey's 2004 book *Digital Evidence and Computer Crime*[58] contains a section that explains how to perform a forensic analysis on Usenet;[59] however, Internet service providers have not offered access to part or all of the Usenet hierarchy for the past few years.[60] As a result, a government analyst, who spent time learning this technology, now has no use for that skill set and instead must retrain in order to learn the new technologies that are growing in popularity.[61] This type of rapid technological change puts pressure

---

based operating systems have been through as many as ten release cycles, depending on the Linux distribution. Ubuntu Releases | Ubuntu, http://www.ubuntu.com/products/whatIsubuntu/releases (last visited Sept. 12, 2009) (showing the release dates for the Ubuntu Linux distribution) (on file with the North Carolina Journal of Law & Technology); Release / Schedule—Fedora Project, http://fedoraproject.org/wiki/Releases/Schedule (last visited Sept. 12, 2009) (showing the release dates for the Fedora Linux distribution) (on file with the North Carolina Journal of Law & Technology).

[58] CASEY, *supra* note57, at 508.

[59] Usenet is a text based Internet protocol centered around the concept of "groups." Users could exchange information by searching for a particular group and virtually congregating with people who are interested in the same topics. The advent of the World Wide Web however led to a sharp decrease in the usage of Usenet. Jeff Tyson, HowStuffWorks: How Newsgroups Work, http://computer.howstuffworks.com/internet/social-networking/information/newsgroup.htm (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

[60] Paul Adams, Verizon Time Warner Cable and Sprint to Block Usenet,—Webmonkey, http://www.webmonkey.com/blog/Verizon_Time_Warner_Cable_and_Sprint_To_Block_Us (last visited Sept. 12, 2009) (explaining how Verizon, Time Warner Cable, and Sprint will no longer provide a way for their users to access Usenet services) (on file with the North Carolina Journal of Law & Technology).

[61] Currently, in much of the world, peer-to-peer ("P2P") traffic makes up over fifty percent of the total Internet traffic. John Timmer, Internet Traffic Report: P2P, Porn Down; Games and Flash up, (Feb. 29, 2009) http://arstechnica.com/web/news/2009/02/internet-traffic-report-p2p-porn-down-games-and-flash-up.ars (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology). The expansion of P2P is fairly recent, gaining popularity around 2000 with the advent of Napster. Jeff Tyson, How the Old Napster

on government computer analysts to be constantly updating their skills to deal with a wide variety of evolving technologies. The Ninth Circuit's electronic search framework, which requires computer personnel to do the initial search of the information,[62] means that since nearly every electronic search will be funneled through computer personnel. These personal will not only have to be up to date on a wide variety of technologies, but will also have more and more cases to process.

2. *Changing the Lineup Card: Handling Technological Evolution within the Ninth Circuit Framework*

One of the primary concerns with the Ninth Circuit's framework is its narrow view of computing. The Ninth Circuit views computing as something that people do within some confined location.[63] This view contradicts the trend of more and more people using what is known as "cloud computing,"[64] a concept that allows one to access his or her data, stored on a central server, from any number of computing devices (various computers, mobile phones, iPods, etc…).[65]

The Ninth Circuit Court appears to have some awareness of issues at least partially related to searches concerning cloud computing, since it mentions that "seizure of . . . Google's email servers to look for a few incriminating messages could jeopardize

---

Worked, http://computer.howstuffworks.com/napster.htm (last visited Oct. 14, 2009) (on file with the North Carolina Journal of Law & Technology).

[62] U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, at *12 (9th Cir. Aug. 25, 2009)

[63] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378 (making no mention of cloud computing, off site backup, or storage).

[64] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.åcom/s3/, (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology); Gmail: Google's approach to email, http://mail.google.com/mail/help/intl/en/about.html, (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology); Getting to know Google Docs, http://docs.google.com/support/bin/answer.py?answer=49008 (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology); KNORR & GRUMAN, *supra* note 9.

[65] *See* KNORR & GRUMAN, *supra* note 9.

the privacy of millions."[66] However, the search framework laid out in *Comprehensive Drug Testing* does not directly address those issues.[67] In addition to not being covered in the Ninth Circuit, electronic search in regards to cloud computing is not being widely addressed in computer forensics texts, federal case law or law journals.[68]

3. *The Big Hitters: Examining Major Cloud Computing Providers in Light of the Ninth Circuit's Framework*

Two examples of popular cloud computing services are Google Docs and Amazon S3.[69] Google Docs is a way for people to write documents, spreadsheets, and presentations without the need for

---

[66] *Comprehensive Drug Testing, Inc.,* 2009 WL 2605378, at *17.

[67] *Id*.

[68] Looking at a variety of computer forensics texts from 2000 from 2004, the term "cloud computing" does not appear in the index of any of them. *See, e.g.*, CASEY, *supra* note 57; EOGHAN CASEY, HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY, (Academic Press, 2002); ROBERT JONES, INTERNET FORENSICS, (O'Reilly Media, 2006). However, the same search conducted on Google News on September 12, 2009 resulted in over 7000 results for the term. A Westlaw search on the term "cloud computing" found two federal cases that contained the term, though neither of them dealt with the concept in regards to the execution of search warrants. (Westlaw, http://lawschool.westlaw.com (search "All Federal Cases" for "cloud computing) (last visited Sept. 25, 2009). Additionally, a Westlaw search for journal or law review articles that contained the term "cloud computing" returned only seventy-eight results. However, once again, none of the results dealt with execution of search warrants for electronic data. (Westlaw, http://lawschool. westlaw.com (search "Law Reviews" for "cloud computing) (last visited Sept. 25, 2009)). This illustrates that though the public media is starting to fully explore the concept of cloud computing, the legal world is still only grazing its surface.

[69] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.åcom/s3/, (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology); Getting to know Google Docs: Google Docs basics—Google Docs Help, http://docs.google.com/support/bin/answer.py?answer=49008&cbid=-icsfpx1uzgxw&src=cb&lev=index (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology).

applications like Microsoft Word.[70] Additionally, Google Docs provides a central storage location for these documents so that a user can access the documents from any computing device hooked up to the Internet.[71] Amazon S3, on the other hand, provides inexpensive, off-site backup and storage of information,[72] a service that is useful for individuals who are looking for a way to backup data or for companies who are looking for a way to serve their content via the Internet.[73]

Google Docs allows a user to log into his or her account through a web browser, using a single username and password for all of Google's services, including Google Docs.[74] Additionally, assuming a default configuration, no copies of these documents are stored on the user's computer.[75] How would the framework set out

---

[70] Getting to know Google Docs: Google Docs basics—Google Docs Help, http://docs.google.com/support/bin/answer.py?answer=49008 (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology).

[71] Google Docs are accessed through a web browser and therefore can be accessed through nearly any device that has web browsing capabilities, including: Android devices, iPhone devices, and Windows mobile devices. Google Mobile Help, http://www.google.com/support/forum/p/Google+Mobile (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

[72] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3/ (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology).

[73] *Id.*

[74] More Google Products, http://www.google.com/options (last visited Oct. 23, 2009) (listing services that can be accessed with a Google account) (on file with the North Carolina Journal of Law & Technology); Google Accounts, https://www.google.com/accounts (last visited Oct. 23, 2009) (showing the login screen for a Google account and listing some of the available services that can be accessed with such an account) (on file with the North Carolina Journal of Law & Technology).

[75] An end user could use a different method of access to their Google data, such as IMAP for Gmail, that would allow the user to copy a section of the data to his or her hard drive. Enabling IMAP—Gmail Help, http://mail.google.com/support/bin/answer.py?hl=en&answer=77695 (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology). Additionally, a user could use the "Google Gears" service to create local offline copies of his or

by the Ninth Circuit in *Comprehensive Drug Testing* be applied to this type of structure? The Ninth Circuit's framework was based on Professor Clancy's "container approach,"[76] but what, in regard to Google Docs, is the actual container? Is it the suspect's Google Docs account? Is it the suspect's Google account generally? Is it the entire Google server system? This question about container size, as the Ninth Circuit briefly alluded to, has wide reaching privacy implications.[77] The framework, as written, leaves open the possibility that a single warrant for one user's account could be enough to give the government's computer personnel the authority to copy the entirety of the Google data stores to another facility to sift through the totality of its data[78].

Amazon S3 is slightly more complicated than Google Docs to access. Instead of simply using a web browser to access the site, Amazon S3 requires a piece of client software[79] that accepts a 12 digit authentication code, email address, and password.[80] Though this initial barrier to entry might make the process of getting data onto servers slightly more complicated, once the data is in Amazon's facilities, similar issues as discussed with Google Docs

---

her data to store locally. General Info: About Gears—Gears Help, http://gears.google.com/support/bin/answer.py?hl=en&answer=79873 (last visited Oct. 23, 2009) (explaining the functionality of Google Gears) (on file with the North Carolina Journal of Law & Technology).

[76] *See* CLANCY, *supra* note 6, at 261.

[77] U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, at *14 (9th Cir. Aug. 25, 2009).

[78] *See* discussion *infra* Part II.C for a full enumeration of the Ninth Circuit's electronic search framework.

[79] Panic—Transmit 3—The next-generation Mac OS X FTP client, http://www.panic.com/transmit (last visited Nov. 3, 2009) (showing an example of a client for Amazon S3) (on file with the North Carolina Journal of Law & Technology) Jungle Disk—Reliable online backup and storage powered by Amazon S3, http://www.jungledisk.com (last visited Nov. 3, 2009) (showing an example of a client for Amazon S3) (on file with the North Carolina Journal of Law & Technology).

[80] Amazon S3—The Beginner's Guide | How To, http://www.hongkiat.com/blog/amazon-s3-the-beginners-guide/ (last visited Nov. 3, 2009) (on file with the North Carolina Journal of Law & Technology).

arise.[81] The most important of these issues is determining how big of a "container" the warrant should cover. The data container issue can be further complicated due to the use of redundancy that Amazon S3 employs regarding the storage of each user's data.[82]

4. *Updating the Box Score: Examining Internet Archival Services with Respect to the Ninth Circuit Framework*

In addition to online storage solutions designed for individuals to back up personal data, there are also websites whose purpose is to archive the Internet itself. The most prominent of these sites is The Internet Archive[83], which is most commonly referred to by its uniform resource locator ("URL") "archive.org."[84] This site allows people to view what a particular website looked like on a given

[81] *See* discussion *infra* Part.II.E.3.

[82] Each person's data is stored in at least two physical locations spread throughout the United States. Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3/ (last visited Nov. 3, 2009) (on file with the North Carolina Journal of Law & Technology). The fact that data is available in two locations creates new questions concerning the scope of the original warrant. For example, does the warrant cover all the locations that the user's data is located, could be located, or has been located? The Ninth Circuit framework does not address this issue. For more discussion about the necessity for data redundancy in off-site cloud storage, *see* Roy Furchgott, The Beauty in Redundancy, http://gadgetwise.blogs.nytimes.com/2009/10/12/the-beauty-in-redundancy/ (last visited Oct. 23, 2009) (explaining why it is important that cloud data be stored in a redundant manner to prevent issues such as those which occurred recently when users of the T-Mobile Sidekick lost all of their online data) (showing the login screen for a Google account and listing some of the available services that can be accessed with such an account).

[83] Internet Archive: About IA, http://www.archive.org/about/about.php (last visited Sept. 25, 2009) (on file with the North Carolina Journal of Law & Technology).

[84] Archive.org states that "[i]ts purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format." *Id.* They accomplish this by creating another copy of web content and storing it along with the date the item was archived to allow people to create what archive.org calls a "way back machine" that allows people to view what a particular website looked like on a given day. Internet Archive Frequently Asked Questions, http://www.archive.org/about/faqs.php (last visited Sept. 25, 2009) (on file with the North Carolina Journal of Law & Technology).

day.[85] Though the number of hypothetical situations that can be extrapolated from this type of service is limited only by imagination, consider the situation where an Internet user posts something to his or her blog that is in fact a crime but then later decides to remove the post. Can the government submit a search warrant to archive.org to find the particular version of the Internet user's website that contains the materials that violate the law, even though the user has rectified the situation? This type of discussion can lead to a whole realm of issues[86] that are beyond the scope of this Recent Development and, also, not accounted for in the Ninth Circuit's framework.[87]

5. *Instant Replay: Discussion About Whether or not Search Warrants Are Required in Cloud Computing Searches*

Before examining an application of the Ninth Circuit's framework in regards to cloud computing, a brief discussion about whether search warrants apply to this type of off-site storage is required. The cases that deal with the application of physical search rulings to electronic search activities are sparse[88] and currently the question about the appropriate instrument for searching of offsite data storage is in the realm of academic debate.

---

[85] *Id.*

[86] For example, in the recent MySpace bullying case, a mother created a MySpace profile to harass one of her daughter's friends and said friend later committed suicide. Judge Tentatively Acquits Missouri Mother in MySpace Hoax Case, Jul. 2, 2009, http://www.foxnews.com/story/0,2933,529817,00.html (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology). What if the mother decided to remove the MySpace page before her daughter's friend even saw it but later her daughter's friend found a copy of the page in the Internet Archive and, as a result of seeing this archived copy of the page, committed suicide? Is the mother just as responsible as she was when her daughter's friend saw the actual MySpace page? Is there now a liability issue with the Internet Archive for revealing this deleted page to the daughter's friend?

[87] *See* U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, at *14 (9th Cir. Aug. 25, 2009) (lacking any mention of the contents of independent in Internet archiving, search engine caching or website metadata storage).

[88] Orin S. Kerr, *Digital Evidence and the New Procedure*, 105 COLUM. L. REV. 279, 293 (2005).

Professor Christopher Slobogin[89] has made the case that instead of a search warrant; all that is required for access to third party electronic data stores is a grand jury subpoena.[90] Professor Slobogin's analysis starts with the Supreme Court's decision in *Katz v. United States,*[91] continues on to the holding in *United States v. Miller,*[92] and then concludes with two applications of the *Katz* and *Miller* holdings in lower court decisions concerning electronic

[89] Professor Slobogin was a member of the America Bar Association's task force on transaction surveillance. UF Levin College of Law | Faculty and Staff, http://www.law.ufl.edu/faculty/slobogin/ (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

[90] *See generally* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK, (The University of Chicago Press 2007) (arguing that searching a third party data storage location amounts to "transactional surveillance" and therefore does not require a search warrant but merely a grand jury subpoena).

[91] *See* Katz v. U.S., 389 U.S. 347 (1967) (holding that a man who makes a phone call from an enclosed phone booth receives Fourth Amendment protection even though the phone booth is located in a public place). The key quotes from this opinion relevant to the issue of third party data storage are: (1) "the Fourth Amendment protects people, not places" and (2) "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351. Though this is only the first step in the analysis of third party data stores, it provides the foundation that the rest of the analysis is built upon. When using a system like Google Docs or Amazon S3, a user provides authentication information, *see* discussion *supra* Part II.E.3, in order to ensure that his or her information is private. In other words, he or she "seeks to preserve [the information] as private" as required by *Katz. Id.*

[92] *See* U.S. v. Miller, 425 U.S. 435 (1976) (holding that personal bank records that have been given over to a bank and are used for the bank's record keeping purposes are not subject to Fourth Amendment protection). The key question that the Supreme Court asked in *Miller* was "whether there is a legitimate expectation of privacy concerning [the record's] contents." *Id.* at 441. The Court found that checks and deposit slips that were "negotiable instruments to be used in commercial transactions" and as such, were not afforded Fourth Amendment protections. *Id.* However, cloud computing data stores such as Google Docs and Amazon S3 do have an expectation of privacy from their end users. The usage of specific login information is an example of how each individual user is the steward of his or her own files. Additionally, each user can control the visibility permissions of each individual file that he or she creates or uploads. This type of fine grained privacy control is clearly different from handing a bank teller a check or deposit slip and instead indicates that the user has a "legitimate expectation of privacy" concerning his or her stored files.

data.[93] Professor Slobogin's reasoning, though appropriate for some types of electronic data transfer,[94] does not appear to sync well with the concepts of third-party storage in cloud computing, for the principles he outlines seem to push cloud computing data stores into the realm of search warrants.[95] Clearly, until addressed by the courts or by the legislature, there will remain ambiguity as to whether individuals receive Fourth Amendment protection for data they store at third party, cloud computing data stores. For this reason, any new framework, by either the court or the legislature, should clearly state that a person's data, stored at a third party,

---

[93] In PRIVACY AT RISK, *supra* note 92, Professor Slobogin points to two cases to make his point about only a subpoena being required when searching third party data stores: U.S. v. Kennedy, 81 F. Supp.2d 1103 (Kan. D. Ct. 2000) (holding that there was no Fourth Amendment interest for subscriber information that was given over to the ISP) and Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) (holding that information that was given over to the operator of the message board services and information that posted on the public sections of the message board were not subject to Fourth Amendment protection).

[94] The holdings in *Kennedy*, 81 F. Supp.2d 1103, and *Guest*, 255 F.3d 325, deal with subscriber information (such as user name, address, etc.) and data posted on a public section of a computing service. This type of subscriber information is the type of information that *Miller* would view as "lacking a legitimate expectation of privacy." Additionally, the standards for retrieving this information are codified in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)(2) (2006) as lower than that required by warrant. The other type of information that was mentioned in these cases was information that was posted to a public section of an online service. Falling back to the analysis in *Katz*, this type of posting inherently cannot be information the "user seeks to preserve as private," because it is being posted to a public forum. *Katz*, 389 U.S. at 351.

[95] Cloud computing services, such as Google Docs and Amazon S3, require authentication. This shows the user "seeks to preserve [the information] as private." *Katz*, 389 U.S. 347. This argument is bolstered by *Miller*, 425 U.S. 435, which asked the question was "there a legitimate expectation of privacy" concerning the material in question? A user who stores his or her data in a cloud computing data store that is secured by authentication has a clear expectation that this data is private. Additionally, the information stored by in these cloud computing services is more substantial than the basic subscriber information that was requested via subpoena in *Kennedy*, 81 F. Supp.2d 1103, and *Guest*, 255 F.3d 325, suggesting those are not appropriate precedent to follow in this particular situation.

cloud computing data store, is afforded Fourth Amendment protection.

6. *Relief Specialists: How a Framework Should Be Constructed to Handle Cloud Computing*

The primary issues arising out of online services such as Google Docs, Amazon S3, and archive.org[96] are: (1) how to define the "container" that is governed by a particular search warrant, and (2) how to provide that information to the government computer analysts so that they can perform the analysis required by the framework set out in *Comprehensive Drug Testing*.[97]

In the realm of "cloud computing" the container should be defined at the account level. This would mean that, for a Google Docs account, the container would be all data associated with a particular e-mail address and password combination[98] and, for an Amazon S3 account, a particular authentication code, email address and password combination.[99] The mechanisms by which the government would acquire a specific Internet user's account information are beyond the scope of this Recent Development. Additionally, the container should include any metadata,[100] including editing history, associated with the user's account, thereby preventing a user from temporarily transferring ownership

---

[96] *See* discussion of metadata *supra* note 53.

[97] U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, at *16 (9th Cir. Aug. 25, 2009).

[98] Getting to Know Google Docs: Google Docs Basics—Google Docs Help, http://docs.google.com/support/bin/answer.py?answer=49008 (last visited Sept. 12, 2009) (on file with the North Carolina Journal of Law & Technology).

[99] This account approach could also be applied to any cloud computing service that uses an account based system. Other examples of such services include Dropbox, Dropbox—Tour—Secure backup, sync, and sharing made easy, http://www.getdropbox.com/tour (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology), and MobileMe, Apple—MobileMe—Your iPhone, Mac, and PC. In perfect sync, http://www.apple.com /mobileme/ (last visited Oct. 23, 2009) (on file with the North Carolina Journal of Law & Technology).

[100] *See* discussion of metadata *supra* note 53.

of pieces of digital documentation to a co-conspirator's account outside of the reach of the search warrant.[101]

The issue of how to acquire the container is not as easily solved. There are privacy issues with the government going through the entirety of Google's or Amazon's data stores in order to get one particular user account,[102] in addition to a certain level of expertise required by computer analysts to access certain companies' proprietary storage systems.[103] For that reason, there should be two options for how the government acquires a particular user's cloud computing "container": (1) the company can provide the "container" to the government, or (2) with the company's assistance and permission, the government can extract the "container" itself.

Companies such as Google and Amazon have some of the most visited sites on the Internet,[104] and as a result, have earned the right to be stewards of their own data. As a reward for this success, they should be afforded the opportunity to have their computer analysts extract a particular user's cloud computing "container" and present said container to the government without government involvement.[105] If the government decides that it wants particular

---

[101] If a user originally owned a document and then transferred ownership to another user, then the revision history of that document could be present in the metadata of original user, even though the most recent version of the document was stored in another user's account.

[102] *See* discussion *supra* Part II.E.3 (discussing privacy issues with cloud computing).

[103] For an example of a company's proprietary file system, *see* Dave Hitz, Is WAFL a Filesystem?, http://blogs.netapp.com/dave/2008/12/is-wafl-a-files.html (last visited Oct. 23, 2009) (explaining how Write Anywhere File Layout ("WAFL") is not a true file system) (on file with the North Carolina Journal of Law & Technology).

[104] Alexa Top 500 Global Site, http://www.alexa.com/topsites (last visited Sept. 25, 2009) (showing Google is the number one ranked site and that Amazon is the number twenty-three ranked site) (on file with the North Carolina Journal of Law and Technology).

[105] This is an extension of previous holdings that allowed computer experts to assist in the execution of search warrants. U.S. v. Schwimmer, 692 F. Supp. 119, 126–27 (E.D.N.Y. 1988) (holding that a computer expert is granted statutory authority to execute a search warrant under 18 U.S.C. § 3105 (2006)).

certification or other requirements placed on the individuals who perform this service, then a company like Google or Amazon can market itself as having a "government certified" warrant execution computer analyst on staff. Though there will surely be complaints about the prospect of handing over data to the federal government, the idea that only Google or Amazon employees would be making extractions out of their specific systems should be a positive to interested privacy advocates.

Those companies not large enough to support a warrant execution analyst on staff, or who simply choose not to have such an analyst, would then be required to have a government computer analyst do the extraction. Companies who would like the process to go smoothly would be able to observe and assist the government computer analyst or provide steps for the analyst to follow in performing the extraction required by the warrant execution. Additionally, the ability to allow companies to choose to have their own, on staff, warrant execution analysts also allows the costs of training the personnel to be spread outside of the public sector into the private sector, in exchange for a marketing advantage that companies can use when marketing their services.

III. LAST AT BAT: CONCLUSION

The framework set forth by the Ninth Circuit in *Comprehensive Drug Testing*[106] establishes the way the government must execute search warrants on electronic data in the quickly evolving world of computing technology.[107] The framework does have some positive elements, such as its usage of the "container approach"[108] and its lack of particular file type or file name restrictions.[109] Its key flaws, however, are its lack of accounting for the rapid evolution of computing technologies[110]

---

[106] U.S. v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, (9th Cir. Aug. 25, 2009).

[107] *See generally id.*

[108] Clancy, *supra* note 6, at 261.

[109] *See generally Comprehensive Drug Testing, Inc.*, 2009 WL 2605378.

[110] *See* discussion *supra* Part II.E.2.

and its lack of accounting for recent computing trends, such as cloud computing.[111] These flaws mean that the framework, as written, is unsustainable going forward. The lack of any standards on how to execute searches in third party hosted cloud computing data stores could lead to warrants for a particular user of a clouding computing service permitting the government to search the entire data set of the entire clouding computing provider. This type of issue would have both lawyers and privacy advocates up in arms.

The rapidly evolving computing landscape calls for expansion upon the principles set forth by the Ninth Circuit[112] and the creation of a framework that can last in the face of trends such as cloud computing. This framework should include an updated version of the "container"[113] approach to electronic search and define a container for cloud computing services at the user account level. The framework should also allow companies to extract the user data themselves and present it to the government instead of always requiring government computer personnel to execute the search warrant on third party computing services. Finally, the framework should make it clear that a user's data stored in a third party clouding computing data is entitled to full Fourth Amendment protections, eliminating an debate as to whether or not an individual's data could be retrieved merely with a grand jury subpoena.[114] A framework that encompasses these elements would provide lasting privacy protections for individuals in a world of rapid technological evolution.

---

[111] *See* discussion *supra* Part II.E.3.

[112] *Comprehensive Drug Testing, Inc.*, 2008 WL 2605378 at * 17.

[113] Clancy, *supra* note 6, at 261.

[114] *See* discussion *supra* Part II.E.5.