Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 January 2010
Draft

Discussion paper

Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"

Prepared by
Joseph J. Schwerha IV
TraceEvidence, LLC

Project funded by Romania, Monaco, Estonia, Microsoft, McAfee and the Council of Europe

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Disclaimer

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the parties to the instruments referred to

Contents

1 Introduction[1]

Today, cybercrime is a real threat to individuals, businesses and governments throughout the World. And as information technology has advanced, the opportunities to commit cybercrimes over vast distances have increased concurrently. Fortunately, the Council of Europe proactively addresses these threats by producing its Convention on Cybercrime. Almost eight years after this convention started, one can see it has had success at both drawing attention to cybercrime, in general, and helping to solve old and emerging issues inherent in the prosecution of same. One of the emerging issues beginning to draw increased attention is the international acquisition of evidence from cloud computing providers, which I define as including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), as well their deployment models (collectively Cloud Computing Providers).

Many companies have begun to use cloud computing providers in order to control their data, make it universally available, and to minimize their information technology costs. Cloud computing comes in various incarnations, however, with differing popularity. For example, consider one of Google's major initiatives: Google Docs®. This service not only allows for remote storage, but also executes all word processing tasks through a web browser. In September 2009, it was reported that there were around 4.4 million visits to Google Docs2. Web-based email systems are another example of cloud computing. It would appear that the number of user accounts of web-based email services is now well over 200 million. Further, as more employees have begun to work some portion of their workweek from their homes, there has been a measurable increase in the usage of online back up and synchronization services. Instead of hunting and hoping to find that one file on your work, home or spare personal computer, now you just look to your online solution, such as Carbonite® or Mozy®. Undoubtedly the players will change; but, the concept of outsourcing storage and computer processing is not going away. The array of cloud computing offerings is only going to increase.

International cybercrime has been viewed as a growing issue by many entities.3 At least one scholar has broken them down into four categories: "professional law enforcement efforts, regional efforts, multinational efforts, and global international efforts."4 Examples of professional law enforcement efforts include organizations with the prevention of cybercrime as one of their primary goals, such as Interpol and Europol.5 Similarly, there are global efforts, such as the United Nations' International Telecommunications Unions Global Cybersecurity Agenda.[6]

For many nations, international cybercrime and investigation is more important than purely domestic cybercrime and investigation. For example, it has been claimed that over 80% of

1This white paper was produced Joseph J. Schwerha IV, through TraceEvidence, LLC. It was drafted for the Council of Europe, under its Global Project on Cybercrime in order to further international discussions on the security and privacy of cloud computing. The opinions presented herein are solely that of the author, and do not necessarily represent that of any governmental entity of the United States, nor of California University of Pennsylvania.

2 http://blog.compete.com/2008/11/13/google-docs-spreadsheets-microsoft-office/.

3 See. Shannon C. Sprinkel, Global Internet Regulation: The Residual Effects of the "ILOVEYOU" Computer Virus and the Draft Convention on Cyber-crime, 25 Suffolk Transnat'l L. Rev. 491 (Summer, 2002).

4 International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene, Xingan Li, Webology, Vol. 4, No. 3 (September 2007)

5 Id.

6 See ITU Toolkit for Cybercrime Legislation, United Nations Cybersecurity Programme, American Bar Association's Privacy & Computer Crime Committee, Section of Science and Technology Law (Nov. 2008), and Understanding Cybercrime: A Guide for Developing Countries, pp. 212-213, ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunications Development Sector (Draft April 2009).

the cybercrime in Germany is international in nature.[7] This concern with international cybercrime has lead to several efforts to address international cybercrime as a problem, including development of: the 2002 OECD "Guidelines for the Security of Information and Networks: Towards a Culture of Security" setting forth appropriate principles; the Council Framework Decision on Attacks Against Information Systems to harmonize EU cybercrime law; the G8 Ten Principles to Combat High-Tech Crime and the Action Plan to Combat High-Tech Crime; the APEC Telecommunications and Information Working Group; and, APEC-ASEAN Joint Workshop on Network Security.[8] As the globe becomes progressively more interconnected, there is little double that law enforcement authorities will be looking abroad more often.

2 Council of Europe Convention on Cybercrime: Overview

On the cusp of the dawning of the recent millennia, the Council of Europe ("COE") succeeded in drafting and opening for signature the first true international treaty that sought to address the emergence of new types of crime by means of new computer and Internet technologies.[9] The birth of the Convention on Cybercrime was gleaned from the mutual recognition of a need for "co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies."[10]

The Convention on Cybercrime was conceived in Strasbourg, France, with the active participation of the COE of Canada, Japan, South Africa and the USA. After four years and twenty-seven drafts[11], the then forty-one nations Council of Europe adopted the Convention on Cybercrime on November 8, 2001.[12] The Convention was opened for signature in Budapest, on November 23, 2001. Thirty countries signed the Convention (including four non-members of the Council of Europe which participated in the negotiations: Canada, United States, Japan and South Africa).[13] By August 2009, 46 Countries have signed and 26 have ratified[14] the Convention on Cybercrime.[15]

The Convention is intended to be the "first international treaty on crimes committed via the Internet and other computer networks."[16] Its provisions particularly deal with infringements of copyrights, computer-related fraud, child pornography, and violations of network security.[17] Its main objective, set out in the preamble, is to "pursue . . . a common criminal policy aimed at the protection of society against cybercrime . . . especially by adopting appropriate legislation and fostering international co-operation."[18]

The Convention is broken up into four main chapters, with each segment consisting of several articles.[19] The first chapter defines the terms commonly used in cyber technology

7 Transborder Search: A New Perspective in Law Enforcement, Seitz, 7 Yale J. L. & Tech. 23 (2005).

8 List compiled by ITU Toolkit for Cybercrime Legislation, United Nations Cybersecurity Programme, American Bar Association's Privacy & Computer Crime Committee, Section of Science and Technology Law (Nov. 2008)

9 Henceforth, this shall be referred to as "cyber" technology.

10 See Council of Europe Convention on Cybercrime (signed 23 Nov. 2001).

11 Russell G. Smith, Cyber Criminals on Trial (Cambridge University Press, 2004)

12 Convention on Cybercrime

13 Id.

14 Serbia ratified the Convention in August of 2009

15Council of Europe, Chart of Signatures and Ratifications at
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=7&DF=07/01/2010&CL=ENG

16 See Convention, generally.

17 Id.

18 Id., Preamble

19 With Exception to Chapter 1

and may have lead to ambiguity if left undefined.[20] The second chapter outlines the substantive criminal laws and the common legislation all ratifying countries must adopt to prevent these offenses.[21] The second chapter also frames the procedural requirements to which individual States must adhere. The third chapter contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties and where such a basis exists.[22] Finally, the fourth chapter contains the final clauses, including articles pertaining to the signing of the Convention, territorial application of the Convention, declarations, amendments, withdrawals, and federalism.[23]

The Convention aims principally at harmonizing the domestic criminal substantive law elements of offenses and connected provisions in the area of cyber-crime; providing domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses; as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form; and, setting up a fast and effective regime of international co-operation.[24] As such, the Convention defines cyber crime offenses such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighboring rights.[25]

Such is the broad appeal of the Convention. Countries like Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have already drafted parts of their legislation in accordance with the Convention. Although those countries have not yet signed the Convention, they are supporting the harmonization and standardization process intended by the drafters of the Convention.[26]

3 What are Cloud Computing Providers?

Before we further assess and analyze international acquisition of evidence to support cybercrime investigations, it is important to more precisely define "Cloud Computing Providers." "Cloud Computing" is a simple term used to refer to a complex paradigm of functions that has yet to arrive at a precise definition. The Internet has been long deemed "the cloud" for the cloud diagram used to represent its networking infrastructure, and "computing" somewhat vaguely indicates the use of remote functionality online. At its most basic, cloud computing describes the act of delivering hosted services over the Internet. While at its most complex, cloud computing extends to abstract functions that have yet to be realized. The most precise definition of cloud computing may by the delivery of computational services through network architecture that allows users to access remote services on demand, while those services primarily are managed by the third-parties. Three major categories have been defined for the types of services provided by cloud computing:

20 Convention, Explanatory Report. "It was understood by the drafters that under this Convention Parties would not be obliged to copy verbatim into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation."

21 Id., Convention.

22 Id.

23 Id. Art. 41 (Federal Clause).

24 Explanatory Report, para. 16

25 Convention, Arts. 2 – 10.

26 See Gerke, Marko, Understanding Cybercrime: A Guide for Developing Countries, ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunications Development Sector (Draft April 2009).

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

IaaS is used to provide virtual servers to customers in a model in which customers pay for what is used. IaaS is also called "utility computing" because of its payment system, which is similar to the consumption of natural resources. For example, Amazon Web Services, arguably the largest IaaS system, supplies users with unique IP addresses and blocks of storage on demand. Organizations using IaaS outsource the equipment used to support operations to a service provider, who is then responsible for distribution to consumers. Some of the benefits include dynamic scaling, usage-based pricing, reduced costs, and access to superior information technology resources.

PaaS is used to host software and product development tools, but unlike IaaS, consumers of PaaS develop applications themselves which may be forced to remain on the provider's platform. PaaS enables operating system features to be changed or updated frequently, and delivers its services online without downloads or installation. PaaS is also known as "cloudware" for its capability of delivering resources from private computers to the Internet. Some of the benefits of PaaS include multi-tenant development tools, deployment architecture, and integrated management and billing.

Finally, SaaS is the delivery of software over the Internet. It is used to provide consumers with hardware infrastructure and software through a front-end portal that enables users to access the service anywhere, such as webmail. As opposed to purchasing highly costly software, companies or individual users can license a single version of a product online. SaaS includes many other benefits, such as easier administration, automatic updates, compatibility among users, and global access.

Cloud computing in the mainstream is called a public cloud, meaning that applications and services are shared online to the general public by third parties. A public cloud is the standard model of cloud computing. In contrast, a private cloud provides an internal service inside the consumer's datacenter that is managed by the consumer. Services are hosted to a limited number of people behind a firewall, and enable consumers to exercise more control over their data. Generally, public clouds are more cost effective and efficient in the short-term, while private clouds enable companies to increase security and expertise of the program. As a final alternative, hybrid clouds employ both public and private models, enabling companies to use a public cloud service for general computing, while keeping customer data within its private cloud. A hybrid cloud may be the best option for organizations, and is gaining popularity with large companies. For example, HP's latest version of its Operations Orchestration software allows companies to standardize provisioning and de-provisioning workflows on both public and private clouds through automation.[27]

Cloud computing is an advantageous alternative to traditional business software, providing a cost-effective method for businesses to employ up-to-date applications, without the financial strain of paying for programs that aren't used or burdening in-house IT departments which could be otherwise be allocating limited resources on new projects. However, while cloud computing may be highly beneficial to users, limitations such as security risks and lack of legal understanding can pose challenges to law enforcement and counsel involved in e-discovery. Data used in cloud computing is constantly in transit, thus constraining document preservation and potentially impeding evidence collection.

27 An emerging trend in cloud computing is that of the community cloud. Community cloud computing involves sharing resources by several organizations with a common purpose that can be managed by a third party or the organizations themselves. See www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

4 The United States Perspective

In the United States, we are bound by both federal and individual state-based laws.[28] Indeed, criminal investigation generally are prosecuted by a by a United States Attorney, State Attorney General or District Attorney. The former prosecutes under Federal law, whereas the latter two prosecute under the individual state's criminal laws and procedures in which that entity is located.[29] While federal prosecutors may be able to utilize procedures for searching across state lines, a typical state-based prosecutor largely only has tools based in the state rules of criminal procedure for their own state.[30] Typically, the state procedural rules do not allow for the direct acquisition of evidence from a location outside of a state.[31] It can be very difficult to understand and comply with each state's laws with respect to acquisition of digital evidence across state lines. While we do have a federal law that would apply in every case, some state laws are more restrictive and; therefore, must also be complied with on a case-by-case basis.

One may look to how local and state authorities within the United States have dealt with acquisition of electronic evidence across state lines as an analogy to how countries may decide to deal with this issue at the international level. The analogy is applicable in some respects and does not hold in others. It is true that the primary methodology for acquiring digital evidence within a particular jurisdiction remains a search warrant or other associated orders.[32] However, if the requesting authority is not an entity that can take advantage of federal jurisdiction, as such is the case generally for all local and state authorities within the United States, the requesting authority will only have the ability to compel production of digital evidence from a third party physically located within the requesting party's state. This begs the question as to how such authorities investigate cases involving evidence from other states. In that circumstance, the investigative authority has a choice.[33] They can go to the repository state and seek help from the local law enforcement authorities to acquire it. They could also directly serve the out-of-state provider with the appropriate documents as if that provider was located within the requesting authority's jurisdiction. Many out-of-state providers will honor that request, because they actually are subject to process within the requesting party's state by virtue of agreeing to said situation by being granted a privilege to do business within the requesting party's state.[34] The latter situation has drawn some scrutiny; but has never been deemed to be illegal.

---

28 See Westby, Jody R. Ed., International Guide to Combating Cybercrime, pp. 136 – 137, American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law (2002), as well as the best practice guides cited therein.

29 For instance, a computer intrusion within the state of Pennsylvania could be prosecuted by a representative of the State Attorney General's office, or by a representative of a District Attorney within a county that would have jurisdiction to prosecute the offense. Moreover, both have concurrent jurisdiction to prosecute most cybercrime violations under Pennsylvania criminal law, such as 18 Pa.C.S.A. § 3911.

30 For instance, an Assistant District Attorney can have an investigating officer serve a search warrant only within the confines of their particular state.

31 There is an exception to this principle under 18 U.S.C. § 2703(d), which allows for state investigators to use a Federal law to further their state criminal investigations.

32 Under the Federal Rules of Criminal Procedure, a party seeking to compel information with regard to stored electronic communications held by a provider to the public, the party may utilize a search warrant, a specific and articulable facts order, or a subpoena.

33 This also assumes that they are not prosecuting a case at the Federal level at the same time.

34 The particular tools used will depend upon several factors, including whether the subject of the search is "(a) voluntary or compelled disclosure of information (b) by an "electronic communication service" or a "remote computing service" (c) that offers services "to the public" or not (d) of the "contents of communication" or of noncontents; and (e) of communications that are in "electronic storage" or in transit." Omer Tene, What Google Knows: Privacy and Internet Search Engines, 2008 Utah L. Rev. 1433, 1476 (2008).

About five to ten years ago, there was some controversy over the proper methodologies to be used to acquire both content and non-content information from online web-based, email providers, such as yahoo or hotmail.[35] Previous to that, emails were primarily found on the local personal computer being searched. However, once people started using web-based email, this was not necessarily the case. Instead, the law enforcement investigation team would have to seek disclosure of the emails and their metadata from the email provider itself. The question was whether or not legal process in the territory seeking the information (i.e. where the crime was committed) was applicable. The alternative was going to try and acquire or utilize the requisite procedures in the jurisdiction where the information physically was located. This situation is directly applicable to the current topic of this paper since web-based email is a great example of several types of Cloud Computing Providers (i.e. Infrastructure-as-a-Service and Software-as-a-Service). On the international level, the issues are much more complex.[36]

5 What are the challenges in the transnational acquisition of evidence from Cloud Computing Providers?

There are numerous issues that are directly applicable to the transnational acquisition of evidence from Cloud Computing Providers. In order to structure discussion and simplify the analysis, I will only discuss the more salient issues, as follows.

5.1 It can be impossible to know where the data resides

In the Cloud Computing scenario, the sought after data likely will be stored remotely at a server under the dominion and control of the Cloud Computing Provider. However, even if the investigating officer becomes aware of the provider of the services, it may very well be impossible for that officer to know in what jurisdiction said information actually resides. For example, if you know that the suspect is using Google Docs®, you may think the information is located within the United States. However, I suspect in order to have a more prompt service, said Cloud providers will be tempted to store the client's data closer to the end user. Consequently, Google might store European user data within the European Union even though Google is an American-based company. If an investigation officer wants to preserve data by going directly to law enforcement in the repository country, how would a typical officer proceed in my example? I suspect that you would be forced to contact Google directly in order to find the jurisdiction containing the actual data. However, some commentators may consider that contact to be a search. So the lowly law enforcement officer may be forced to do a kind of transborder investigation, or search, in order to find out even in what jurisdiction the data actually resides. And if the officer can find out where the data resides, then said officer would then have to decide on the best and most appropriate way to preserve and acquire that data, which includes the analysis stated elsewhere herein. Thus, such as in other international investigations, the investigating officer can easily be put in a situation where it is impossible to investigate a transnational cybercrime if the officer cannot do any search or investigate beyond his country's borders without specific involvement of the law enforcement authorities in the country within which the sought after data resides.

Another problematic scenario will be where the Cloud Computing Provider is not able to state specifically in what jurisdiction the sought after information resides. Data storage can be a

35 The tools used depend upon many factors, which are not always easily defined. See What Google Knows, supra.

36 There is much discussion of these scenarios at the international level. See, International Guide to Combating Cybercrime at 154.

complicated proposition. Businesses in this arena take many steps to ensure both the security and availability of data stored on their networks. It is not uncommon for client data to be stored in more than one physical space, or even multiple countries. If a Cloud Computing Provider attempts to preserve data at the request of law enforcement, they may be searching a database without the ability to state exactly from where the data is being drawn.[37] In that case, complications will obviously arise as to compliance with said jurisdictions privacy laws.

As Cloud Computing becomes more regular, it is possible that the ability to gain evidence by merely searching the computing devices possessed by the suspect will greatly decrease. By definition, Cloud Computing Providers are storing the sought after data. While there likely could be trace evidence of having utilized a specific provider, as people start to move towards Cloud Computing, the data will not reside on the individual computing devices held by the suspects. It is equally possible; however, that there will not be even trace evidence of such usage. One of the world's most popular browsers, Internet Explorer from Microsoft allows for "InPrivate" browsing that, at least allegedly, does not leave any trace of the computer user having gone to any particular web site.[38] I suspect that there are other plug-ins for other browsers that do the same thing. Thus, many investigations may not produce evidence on the suspect's custodial computing device that would show evidence of criminal activity.

5.2 What Law Applies When You Do Not Know Where Data Was Stored

If you do not know where the suspect's data was stored, you cannot verify that it was acquired legally.[39] In many common law countries, law enforcement authorities must be able to verify that they have gathered evidence in a lawful manner.[40] In some circumstances, law enforcement authorities may be forced to gather evidence from cloud computing providers without knowing for certain where the evidence resides. This situation likely would not occur if the investigative agency is able to work with law enforcement from the country where the data was stored. In that case as long as the provider itself knows the exact jurisdiction in which the data resides, the requesting authority would be able to verify the legality of the collection under both the investigating authority's substantive and procedural law, as well as the country's law where the data is gathered from. However, should the investigative authority be forced to use self-help to gather the evidence itself, either with or without the appropriate consent, then it is likely that the gathering authority would not be able to verify that the collection was done in accordance with the law of the country from which the data was actually stored. You just cannot verify what you do not know.

37 This is going to be dependent upon the enterprise system architecture, and very well could change over time. Since systems could be using caching servers transparent to the end user, the person at the keyboard may not know where the actual data is coming from exactly.

38 See http://www.microsoft.com/windows/internet-explorer/features/safer.aspx. The feature is described as follows by Microsoft: "When checking e-mail at an Internet café or shopping for a gift on a family PC, you don't want to leave any trace of specific web browsing activity. InPrivate Browsing in Internet Explorer 8 helps prevent your browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, leaving no evidence of your browsing or search history."

39 Many countries view electronic privacy and crime differently. For instance, when writing about Hong Kong, one author has written that "[e]lectronic privacy is a moral concept." See also Kam, Wong, Computer Crime and Control in Hong Kong, 14 Pac. Rim L. & Pol'y 337, 345 (April, 2005)

40 For example, in the United States, a defendant could challenge the process by filing a Motion to Suppress said evidence. This is exactly what was done in the Gorshkov case discussed herein. See U.S. v. Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001).

In similar circumstances, some United States law enforcement authorities are recommending obtaining a search warrant for the seizure only by virtue of direct acquisition.[41] Said advice includes a warning that the investigating officer could be subject to arrest if said search violates a foreign jurisdiction's laws. This is not necessarily a good solution, and certainly demonstrates the difficulty of the present situation with regard to Cloud Computing Providers.

5.3 Getting Data via Consent Creates Many Issues

By virtue of the Convention and other international documents, there is a delineation made as to the legality of the transborder search dependent upon whether appropriate consent was given. For instance, under Article 32(b) of the Convention, the investigative authority may perform a transborder search if the "the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system" is obtained.[42] Because such provisions are not specific in many respects, the whole idea of consent gets murky when dealing with cloud computing providers.

If getting consent is the difference between a legal and illegal transborder search, one must question who is actually able to consent? For example, an employer may be investigating whether an employee is improperly writing computer code for his own personal company while being paid by his employer for employer-related tasks that are not being performed. The employer wants to know when the employee logged into the employer's SaaS account, which just happens to be located in another country. If the employer reports this suspicious activity to law enforcement, and those officials believe that they need consent to immediately retrieve information from the SaaS provider, whose consent do they need? One would think that consent of the employee would be one choice. In some jurisdictions, like the United States, it is the employer who could provide consent. However, a representative of the SaaS provider might also be able to consent, depending upon whether doing so is addressed in its terms of service. For example, if a suspect was utilizing Google Docs® for a SaaS provider, then said suspect would necessarily have to agree to its terms of service. Through using its services a Google user agrees to its Privacy Policy. In pertinent part, Google's Privacy Policy discusses information sharing under a section with that same title, including in relevant part:

> Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:
>
> - We have your consent. We require opt-in consent for the sharing of any sensitive personal information.

41 One inquiry to a law enforcement official resulted in them revealing the wording of a memorandum that they have recently distributed regarding this topic:

"_____ recommends identifying the remote storage provider and using appropriate process to compel the production of the stored files. The problem, of course, is identifying the service provider pre-search warrant. Another approach is to request in your search warrant authorization to preserve these records if discovered. In short you are using the exigency exception to the search warrant requirement to preserve the records. The key points that one needs to be aware of are:

1. Your seizure is based the exigency exception to the warrant requirement. If you learn during the search that these records can be protected and preserved by the 3rd party storage provider your exigency ceases to exist and you must go through the 3rd party provider to obtain the records.
2. If you choose to seize the records you must only make a copy (do not remove or delete the original)
3. Once you have the copy you must reapply with the court (piggyback search warrant) to examine these records.
4. WARNING: if the records are stored outside of the United Sates you run the risk of violating a foreign jurisdictions computer crime laws and may be subject to arrest."

42 Council of Europe Convention on Cybercrime, Article 32.

- We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.
- *We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.* (emphasis added)[43]

It would appear that Google could consent to disclose the content of a user's account without said user's consent under a wide variety of circumstances. It would also seem logical that this circumstance would extend the controversy over whose consent is necessary as at least two entities (Google and the user) could actually consent to the distribution of information contained within the suspect's account.

As with all investigations, a primary concern about basing your authority to search upon consent is that consent usually can be withdrawn. Again, in this case we are assuming that the validity of a transborder search depends upon the prior obtaining of the appropriate consent. However, as easy as it can be to get consent, it is just as easy to withdraw same. Should the consent be withdrawn, what can the investigative officer do? What about irrevocable consent?

There may be times that consent is needed to legally conduct a transborder search of a cloud computing provider. Even assuming that the law enforcement officer is able to identify the appropriate party from whom to obtain consent, said consent may not be able to be provided. This is not a new concept. Consent has been central to the privacy debate, as well. The one issue, however, is that some commentators believe that you cannot voluntarily give consent to your employer because there is always some form of pressure being exerted by the employer. In those cases, you might not be able to get consent ever, and without regard to what the suspect believes.

5.4 The Data Obtained from the Suspect's Custodial Computer May Have Little Meaning

Traditionally, law enforcement authorities have been able to seize and search evidence within the suspect's disposition and control. Because of the nature of personal computers, if one was seized, law enforcement authorities were able to derive usable information from the user created data found therein. This situation follows because the user created files usually were made or manipulated by a locally-installed software program. However, if law enforcement tries to obtain evidence of value, it may not reside on a custodial computer utilizing a cloud computing provider's services, because any data of evidentiary value would instead be located on the cloud computing provider's servers. It is equally plausible that whatever data is stored locally would not be usable without access to the cloud computing provider's system. What happens if you attempt to open a file without the appropriate program located on your computer? You can't access it. I envision that similar circumstances could play themselves out in upcoming years with respect to searches of users of cloud computing providers' services.

[43] *See* Google's Privacy Policy at http://www.google.com/privacypolicy.html.

5.5 There Could be Significant Evidentiary Issues in Certain Scenarios

Evidence is a complex topic that varies from jurisdiction to jurisdiction.[44] Several concepts do repeat themselves. In order to admit evidence in court, the evidence must be sufficiently reliable. In the circumstance where an officer obtains evidence without the appropriate consent, it may be difficult for said officer to testify as to the authenticity of said evidence. These types of evidentiary issues are not new, and have been the subject of scholarship in the past, under varying circumstances.[45]

Of the various problems discussed above, clearly one of the most perplexing is what to do if you need to immediately preserve evidence stored remotely at a Cloud Computing Provider of unknown location. This is only exacerbated by the notion that in many parts of the world, it is increasingly likely that said Provider would be located in another country. It is thereby imperative that such scenario be discussed further.

6 What Portions of the Convention are Applicable to Transborder Searches

Since this document discusses whether changes need to be made to the Convention in light of the new challenges described above, it is necessary to discuss what provisions of the Convention directly address this issue.

6.1 Review of Article 32

In certain cyber investigations, authorities may only have a limited time in which to access vital data. With such a time table, it is impracticable (in certain situations) to require authorities to navigate through complex diplomatic and legal channels in order to access and obtain essential evidence for a case.[46] The drafters of the Convention recognized the basic need for unilateral transborder access of data in the creation of Article 32.[47]

The text of Article 32[48] addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained appropriate consent. In spite of the Convention's recognition of transborder access to information, practical considerations limit the scope in which unilateral action can be taken. After lengthy discussion, drafters found that such limitation was necessary due to lack of concrete experience on the international level with applicable situations and the overall difficulty in formulating general rules.[49] As such, the final product in regard to Article 32 reflects situations in which all parties agreed that unilateral action are permissible.[50]

---

[44] *See generally*, Stephen Mason, general editor, *Electronic Evidence* (2nd ed., 2010, LexisNexis).

45 See Insa, Fredesvinda (2006), "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting Against High-Tech Crime – Results of a European Study", Journal of Digital Forensic Practice, 1: 4, 285-289.

46 See U.S. v. Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001).

47 Explanatory report, paragraph. 293

48 Article 32 – Trans-border access to stored computer data with consent or where publicly available
"A Party may, without the authorization of another Party:

A. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
B. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

49 Explanatory report, para 293

50 Id. The drafters ultimately agreed not to regulate other situations until such time as further experience has been gathered. As of this date, it is debatable whether such experience has been accrued.

Explicit in the wording of Article 32 (a) of the Convention on Cybercrime, a state may retrieve generally accessible data (open source data) independently of the geographical location of their storage unit without having to ask for the consent of any other state.[51] The thought process behind access to open source data lies within the simple premise that such data is already accessible to the public at large over the internet, and therefore should be accessible to authorities in sanctioned investigations.

Contrasted with the explicit authority imbued in the Article 32(a) for access to open source information, Article 32(b) of the Convention provides that prosecuting authorities are permitted access to stored data in cases of affirmative consent of a legally authorized person.[52] While the Convention itself does offer the exact definition of an "authorized person", the explanatory report allows that the authorized person must be defined according to the respective circumstances and the applicable law of each individual case.[53] Such an example is given within the Article 39 itself, signifying that affirmative consent can be given in situations akin to that of the email service provider who intentionally stores its data in a foreign country. Provided that the service provider has lawful authority to access the data, under the Article they may retrieve the data and voluntarily disclose it to law enforcement officials or permit said officials to access the data.[54] Please note, however, that a country's own laws may be more restrictive. Nevertheless, these persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

It is important to note that no critical reading of Article 32 (b) can offer a basis for the coercion of an authorized person, or foreign entity, to retrieve data from abroad. The Convention explicitly requires consent, which by definition contains an element of voluntariness.[55] As such, through the text of Article 32(b), law enforcement agencies cannot use the power of the Convention to compel an "authorized person", either individual or organization, to provide trans-border data through coercive methods. In such cases, voluntary consent is necessary for the Convention to have any effect.[56]

Finally, it is important to point out that Article 32 does not address the retrieval of not freely accessible data by a prosecuting authority *without the consent* (or even knowledge) of an authorized person or of the affected country. As time passes and the Convention evolves, the future may offer an internationally accepted response to the retrieval of not freely accessible data. However, the current incarnation of the Convention offers no clear answer.

7 Transborder Seizures without Consent under United States Law

The United States has no specific provision allowing or prohibiting transborder seizures of digital evidence of which I am aware. Therein, law enforcement and counsel face numerous challenges in gathering evidence internationally. The first case to utilize extra-territorial seizure, *United States v. Gorshkov*, raises questions of whether such methods could still be

51 See Transborder Search, at p. 6.

52 Council of Europe Convention on Cybercrime, Art. 32B

53 Explanatory Report. Para 294. Also provides the example, "[a] person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article."

54 Explanatory Report, COE Art. 32B, Seitz Article.

55 See Transborder Search, supra.

56 There are issues of what constitutes coercion and consent; however such issues are beyond the scope of this article.

employed almost a decade later. In 2000, Alexey Ivanov and Vasiliy Gorshkov were identified as parties to an elaborate scheme emanating from Russia that had caused the breach of numerous computer systems of United States businesses.[57] The Federal Bureau of Investigation set up a fictitious computer security company called Invita as a "sting" operation. The FBI agents then had the suspects fly to Seattle, Washington, where they engaged in a bogus job interview with the agents.[58] In the course of the interview, Gorshkov was asked to demonstrate his hacking ability using an FBI computer, causing him to access his Russian computer.[59] Both Ivanov and Gorshkov were subsequently arrested, at which time the FBI performed a seizure of the computer used by Gorshkov in his demonstration.[60] The keystroke logging sniffer program used by the FBI exposed the username and password Gorshkov used for his Russian computer, and they logged into the system and downloaded the file contents of the computer.[61] Acting under the supposition that associates of Ivanov and Gorshkov would delete vulnerable evidence on the Russian computers before a search warrant would be procured, the FBI acted before applying for or obtaining the warrant, which was issued on December 1, 2000, ten days after the files had completed their download.[62]

Gorshkov filed a motion to suppress the computer data, and any evidence collected as a result, on the basis that the FBI had performed an illegal seizure.[63] His first challenge was on the basis that the FBI violated the Fourth Amendment by using a sniffer program to obtain his user name and password.[64] Second, he argued that using the password to access Russian computers constituted a violation of the Fourth Amendment as well.[65]

The Defendant's motion was denied for two reasons.[66] First, under the Fourth Amendment, an individual must have a reasonable expectation of privacy for it to have been breached. *Rakas v. Illinois*, 349 U.S. 128, 143 (1978). In this case, the court found that the Defendant could have no reasonable expectation of privacy in the computer supposedly belonging to Invita when the computer was not his, files could be stored, and agents were frequently monitoring his actions while he worked.[67] Second, the Defendant's motion was denied for the exigent circumstances present at the time the FBI accessed his computer.[68]

The court looked to the holding in *United States v. Verdugo-Urquidez* to find that the Fourth Amendment does not protect the rights of individuals abroad in the case of U.S. access of extraterritorial computers.[69] Gorshkov attempted to distinguish the holding in *Verdugo* by asserting that he had voluntarily entered the country, whereas the Defendant in that case had not, arguing that such voluntary entry should create minimum contacts with the U.S.[70] However, Gorshkov's claim that he had established contacts with the U.S. that would render

57 United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, *2 (W.D.Wash. May 23, 2001).

58 Id. at *1.

59 Id.

60 Id.

61 Id.

62 Id.

63 Id. at *1-4.

64 Id.

65 Id.

66 Id.

67 Id.

68See also United States v. Ovidiu-Ionut Nicola-Roman, 2008 WL 6914882 (D.Conn., June 24, 2008)(citing Gorshkov, among other precedent, the court determined that the Fourth Amendment did not apply to a search of a foreign individual conducted overseas.)

69 Gorshkov, supra at *3, citing United States v. Verdugo-Urquidez , 494 U.S. 259 (1990).

70 Id. at *3.

him protected by the Fourth Amendment was unfounded, since his entry into the U.S. was for a criminal purpose and no possessory interest in the data was affected.[71]

On a second ground, Gorshkov endeavored to differentiate his case from *Verdugo* by claiming that the search in *Verdugo* was made lawfully with the consent and authorization of Mexican officials, whereas the search in this case was conducted by the FBI without permission from Russian authorities. Here, the court determined that this claim was irrelevant, since nothing in the *Verdugo* opinion indicated that the reach of the Fourth Amendment turned on this issue.[72] Similarly, Gorshkov's claim that the FBI's actions were illegal based on their failure to comply with Russian law was unfounded since Russian law does not apply to the FBI agents' actions. Simultaneously, the Court found that the FBI sufficiently complied with Russian law. The Electronic Communications Privacy Act and the Wiretap Act could not be used to suppress evidence, as Gorshkov claimed, since neither of these statutes provides a statutory suppression remedy for the FBI's alleged violations.[73] While Gorshkov argued that the FBI seized the data on the Russian computer so that other users would be prevented from accessing it, the court concluded that no user would be prevented from accessing the files.[74] Additionally, the Fourth Amendment protected the agents' right to access the Defendant's computer under a temporary seizure for probable cause when vulnerable evidence was in danger of being destroyed or altered.[7576]

71 2001 WL 1024026 at *3.

72 Id. at *3.

73 Id. at n.4.

74 Id. at n.1.

75 Id. at *4.

76 A few decisions since Gorshkov involving international ediscovery may also assist in looking at the U.S. perspective on transborder searches. In 2007, Columbia Pictures, Inc. v. Bunnell held that a U.S. court with the power to do so could compel a party subject to its jurisdiction to produce evidence. Here, Defendants operated a website that distributed copyrighted material belonging to the Plaintiff online through a peer-to-peer network, and stored much of this information on servers in the Netherlands with the belief that the privacy laws in that country would protect users' identities. No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 (C.D.Cal. May 29, 2007). Defendants in this case argued that they should not have to produce the electronic evidence under Netherlands law, which governed the information on the servers. In reconciling international laws with those of the U.S., the court held that the Defendants could not be precluded from producing the relevant evidence based on three factors: First, over twenty-five U.S. servers were present and the Defendants maintained the ability to control the Server Log Data. Next, it was unclear whether the Netherlands law in question applied to the Server Log Data or the IP addresses used. And third, the court determined that whether or not the Netherlands statute applied, foreign blocking statues cannot prevent an American court from ordering a party subject to its jurisdiction to produce or preserve evidence. Id. at *12. In December of 2007, the case was terminated in favor of the Plaintiffs, based on the Defendants' willful spoliation of evidence. Defendants were found to have willfully despoiled evidence by: Deleting and modifying user forum postings on the website at issue, deleting directory headings referencing the copyrighted works at issue, destroying user IP addresses, and destroying records of the identities and addresses of site moderators. Columbia Pictures, Inc. v. Bunnell, No. 2:06-cv-01093 FMC-JCx, 2007 WL 4877701, at *1-4 (C.D.Cal. December 13, 2007). While it seems fairly clear that U.S. citizens acting abroad can still be required to produce evidence, the sanctions imposed in this case raise questions as to how to enforce the preservation of electronic evidence abroad.

The Bunnell court relied heavily on Richmark Corp. v. Timber Falling Consultants in balancing the interests of foreign and domestic parties in cases of noncompliance with discovery orders based on foreign statutory bars. The Richmark court identified among those factors relevant to deciding whether or not foreign statutes excuse noncompliance with discovery orders: the importance of the documents requested; the degree of specificity of the request; whether the information originated in the U.S.; whether an alternative means of securing the information is available; the extent to which noncompliance would undermine important interests of each country involved; the extent and nature of the hardship that would be imposed on the individual; and the likelihood of compliance. 959 F.2d 1468, 1475-77 (9th Cir. 1992). These factors were again implemented in Synthes (U.S.A.) v. G.M. dos Reis Jr. Ind. Com. De Equip. Nedico in determining whether Synthes was entitled to document discovery from the Defendant, a Brazilian corporation, in the case of patent infringement. No. 07-CV-309-L(AJB), 2008 WL 81111, at *3-7 (S.D.Cal. January 8, 2008). Because the requested discovery was directly relevant to the outcome of the case, the discovery was allowed to the extent of personal jurisdiction, and to avoid conflict with Brazilian law, all depositions of Brazilian nationals were to be conducted in the United States. Id. at *7. Recent rulings, such as this, that compel compliance with international discovery orders can be used to shed light on the question of transborder searches in the wake of Gorshkov. The Richmark factor of whether there exists an alternative means of gathering information is particularly relevant to international electronic discovery where pertinent information may be solely stored online, and therefore more exposed to destruction or alteration. See also Cornwell v. North Ohio Surgical Center, 2009 WL 5174172 (Ohio App. 6 Dist., 2009) and In re Weekly Homes, L.P., 295 S.W.3d 309, 319 (Tex., 2009).

There have not been very many opinions that have cited the Gorshkov case for the proposition of transborder searches. Several commentators have criticized the process, in general. In the International Guide to Combating Cybercrime, the American Bar Association stated that the Gorshkov approach "does not provide a sound basis for transborder searches and seizures because it would inevitably allow one state to transgress upon another state's sovereignty by searching and seizing property belonging to that second state's citizens, property that is physically located within that second state's territory."[77] Further, in the recent draft of the International Telecommunication Union document entitled "Understanding Cybercrime: A Guide for Developing Countries", performing such a search even with consent was criticized, implying not having consent would likewise be questionable at the very least.[78] This methodology appeared to be controversial then and the passage of time has not diminished that prevailing thought.[79]

8 Conclusions

In this white paper, I provided many perspectives regarding the challenges presented in transborder searches and cloud computing. The first portion was devoted to summarizing cloud computing and the issues inherent acquiring evidence there from to prosecute cybercriminals. I then concentrated on one of the most difficult issues, which I defined as transborder searches. One of the overarching principles discussed throughout was the varying methods utilized in the United States and those set forth in the Convention. I will conclude with some specific recommendations and points for further discussion.

8.1 What are the Specific Challenges Presented to Law Enforcement by Cloud Computing?

There are several issues presented to law enforcement by Cloud Computing, including: 1. It is impossible to know where the sought after data resides; 2. If you don't know where the data resides, then you cannot determine what laws apply; 3. The idea that the investigating officer may have to get consent brings about numerous other difficulties; 4. If the investigative authority searches the computer possessed by a suspect that utilizes the services of a Cloud Computing Provider, then any data obtained there from might be meaningless; and 5. There could be significant difficulties in admitting the evidence obtained from a Cloud Computing Provider. Given the complexities of cloud computing, it is likely that there will be other and further challenges, as well.

8.2 Is the Convention Adequate for Transborder Searches?

One of the most difficult issues with regard to acquiring evidence from Cloud Computing Providers to support criminal investigations is obtaining said evidence from such a provider located outside of the investigation officer's country, especially where the investigative officer needs to obtain the evidence as soon as possible. In this circumstance, the officer is faced with the decision of whether or not they can or may acquire said evidence immediately via a transborder search.

77 See International Guide to Combating Cybercrime at 154.

78 See Gerke, Marko, Understanding Cybercrime: A Guide for Developing Countries, pp. 212-213, ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunications Development Sector (Draft April 2009).

79 The inter.net has posed other potential violations of other countries' laws. For instance, by virtue of the global nature of the internet, differing free speech laws poses various potential conflicts of legal regimes. See also Berman, Paul Schiff, The Globalization of Jurisdiction, 151 U. Pa. L. Rev. 311, 337 (December, 2002)("In such circumstances there is an inevitable problem of exterritoriality.")

With respect to transborder searches, one can argue the Convention is both adequate and inadequate at the same time. It is apparent that it does provide some assistance to law enforcement authorities investigating activities on Cloud Computing Providers. Authorities from signatory states certainly can gain access to that information that is "publicly available".[80] This could be applicable to only very general information with respect to how Cloud Computing Services work, in general. For example, an investigating officer could look at advertising literature from Google Docs that is available online. Similarly, that same investigator could lawfully unilaterally access information from a specific account holder, if the investigator had the lawful and voluntary consent of the appropriate party.[81] While it is unlikely that the suspect is going to be that person, it is very plausible that the Cloud Computing Provider would be giving said authority for investigation of activities on that provider's service. One can think of very little reason why Cloud Computing Providers would not have privacy policies like Google's policy, as discussed above. In fact, it has and will be in their interest, to allow law enforcement access to investigate wrongdoings on their systems. Nevertheless, there are so notable issues with Article 32 in its present configuration.

The Convention may not adequately address investigations of a very urgent nature. Under the Convention, an investigator may only perform a transborder search if the information being sought is generally available, or if the investigator has the appropriate consent.[82] Getting consent in extremely time sensitive situations may not be tenable.[83] This difficulty is only exacerbated in scenarios where the evidence being sought is from a Cloud Computing Provider located in a foreign country which may not be easily or quickly accessed through traditional telecommunication methods.

By not directly addressing the situation where a transborder seizure is done without anyone's consent, the Convention invites increased and more vigorous disagreements among signatory nations about the appropriateness of said searches. Some countries, like the United States, will likely follow procedures that they deem appropriate under their own law. Others may be conservative and just not investigate because of possible privacy violations. When those two perspectives clash, the disagreements will be intense. I believe the chance of those arguments only increase as Cloud Computing becomes more popular. I recommend that further discussions be initiated regarding non-consensual transborder seizures.[84]

If further discussions are had, then they should include whether or not there will be a recognized exception for exigent circumstances. Under United States law, there is a recognized exception to the search warrant requirement where exigent circumstances exist. At least one other scholar has indicated that an exception to the principle of territoriality should exist for exigent circumstances.[85] Earlier herein, I discussed various circumstances where the lack of an exception for exigent circumstances might result in the occasional failure of investigative agencies to prosecute international cybercrime. That is an acceptable

80 See Council of Europe Convention on Cybercrime, Article 32(a).

81 Please note that the investigating officer must, of course, also comply with all of their domestic legal requirements.

82 See Council of Europe Convention on Cybercrime, Article 32(a).

83 Please note that the Convention does address slightly less urgent scenarios through its 24/7 points of contact.

84 Professor Susan Brenner has postulated that our model for prosecution of cybercrime may have to change. See Brenner, Susan Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?, 30 Rutgers Computer & Tech. L.J. 1, 104 (2004)("… cybercrime differs in several fundamental aspects from real-world crime, the type of crime which our existing model of law enforcement was developed to address. As a result, the traditional model is not an effective means of dealing with cybercrime.")

85 See Sussman, Michael A., The Critical Challenges From International High-Tech and Computer-related Crime at the Milennium, 9 Duke J. of Comp. & Int'l L. 451, 453-454 (1999).

result if the alternative mandates violation of the principle of territoriality and international law. However, I urge further discussion on this topic in order to seek some middle ground.

One could easily argue that whether Article 32 needs to be modified is a matter of perspective. Getting the agreements necessary to finalize it in its current form was very admirable and solved several issues. However, the lack of specificity with respect to transborder searches without consent would seem to be a significant shortcoming that should be addressed if possible. It is recommended that further exploration should be undertaken to address the points illustrates herein as soon as practicable.

_____