CLOUD COMPUTING & NATIONAL SECURITY LAW

By

The Harvard Law National Security Research Group

Ivana Deyrup & Shane Matthews, Co-Directors

Aatif Iqbal, Benjamin Black, Catherine Fisher, John Cella, Jonathan Abrams, Miranda Dugi, & Rebecca Leventhal

nsrg.hls@gmail.com
TABLE OF CONTENTS

I. EXECUTIVE SUMMARY ................................................................. 3
II. WHAT IS CLOUD COMPUTING? ...................................................... 3
   A. Benefits of Cloud Computing ..................................................... 5
   B. Security Challenges Posed by Cloud Computing ......................... 6
   C. Other Drawbacks to Cloud Computing ....................................... 8
III. LEGAL ISSUES RAISED BY CLOUD COMPUTING RELEVANT TO
     NATIONAL SECURITY AND LAW ENFORCEMENT AGENTS ............ 9
   A. U.S. Laws Criminalizing Harmful Activity in the Cloud .............. 9
      The Computer Fraud & Abuse Act ............................................. 10
   B. Searching & Seizing Information on Cloud Computing Networks ........ 14
      The Electronic Communications Privacy Act ............................. 14
      The Fourth Amendment ....................................................... 16
      The Foreign Intelligence Surveillance Act .................................. 19
   C. Presenting Information from the Cloud in Court ......................... 20
      Accessibility of information stored in the Cloud ........................ 20
      Forensic/Chain of Custody Concerns ....................................... 20
IV. RECOMMENDATIONS .................................................................. 22
I. EXECUTIVE SUMMARY

In recent years, many computer and Internet functions have moved from users’ computers to remote servers that make up a “cloud” of data and processing power. “Cloud computing” has transformed users’ computers from the start and end points of data creation and transmission into portals to view and modify data held under the control of cloud service providers. For example, users of services like Google Docs can create, modify and share access to word processing documents with other users worldwide without ever downloading a single file. The shift to cloud computing has provided a number of benefits, including unprecedented global access to a variety of media, greater scalability, and more efficient use of computing power and customer service resources.

However, cloud computing poses many challenges for U.S. law enforcement and national security agencies. Data aggregated in the cloud is particularly tempting and valuable to hackers. A single cloud service provider’s vulnerability could expose millions of users’ private financial data and other personal information. There is often little indication that such data has been compromised. The patchwork of current U.S. law leaves cloud providers, users and law enforcement with little guidance as to what protections cloud data already has or needs. Jurisdictional questions take on a new dimension in the cloud, as data may be accessed, stored in and transported through multiple locations in several jurisdictions. The same geographical issues may pose problems for law enforcement seeking warrants under the Foreign Intelligence Surveillance Act, where foreign targets may also store data on U.S.-based servers. Cloud computing has made the very definition of what qualifies as “electronic storage” murky under the Electronic Communications Protection Act (ECPA). Courts have yet to determine how many facets of cloud computing will impact Fourth Amendment protections against unreasonable search and seizure, often with jurisprudence lagging far behind the technologies it seeks to address. Finally, cloud-based evidence may pose forensic and chain of custody problems, as accessing cloud data and ensuring it has not been contaminated may be more challenging where there may be multiple, variable storage locations for a single piece of data.

Both the definition of cloud computing and the extent of these security and legal challenges are poorly understood. This report will shed some light on this “cloudy” subject in three parts. First, it will present a definition of cloud computing, examining both its benefits and drawbacks. Second, it will examine legal challenges that cloud computing poses, with particular attention paid to implications of cloud computing for U.S. law enforcement and national security agencies. Third, it will present several recommendations for legislative responses to this new technology.

II. WHAT IS CLOUD COMPUTING?

Simply put, cloud computing allows people to perform computing tasks using infrastructure in remote locations. One familiar cloud computing application is email services like Google’s Gmail, which allows users to access email from any location.
Another example is “Dropbox,” which allows customers to save documents directly to Dropbox’s servers, rather than on their own computers. The customer can access her Dropbox documents regardless of which computer she uses. Cloud computing also allows the Search for Extra-Terrestrial Intelligence (SETI) Institute to use the computing power of volunteers’ personal computers around the world to analyze sounds in outer space through its “SETI at Home” program.[2]

Though the definition of cloud computing is still subject to debate, the U.S. National Institute of Standards and Technology (NIST) has developed a widely accepted definition: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” The NIST definition distinguishes between four types of clouds based on who manages and has access to cloud infrastructure—private clouds (e.g. a single agency), community clouds (e.g. multiple agencies sharing a single cloud), public clouds, and community clouds (e.g. multiple types of independent clouds linked together through proprietary technology).[3] These clouds can deliver services via three models:

- **Cloud Software as a Service**: The consumer uses the cloud network to run a specific computer application, but does not control the infrastructure that runs the application. A popular example is Google Docs, in which users can build spreadsheets or create documents using Google’s software and remote storage space. Google also offers various kinds of business software that is used remotely by start-up companies.[4] Facebook operates similarly, allowing customers to post photos, messages, etc. through a website, while Facebook controls the website and the underlying infrastructure.

- **Cloud Platform as a Service**: The consumer uses the cloud network to create and deliver new electronic applications but does not control the cloud’s infrastructure. One prominent example is Microsoft Azure, which allows users to build and modify applications and then distribute them to customers. For example, the city of Miami used Azure to build a map tracking information about potholes, missed garbage collection, and illegal trash dumping. The city did not have to buy or maintain hardware or software to run the program. Instead, Azure maintained the map.[5]

- **Infrastructure as a Service**: The consumer uses the cloud network to provide the same services as could be accomplished by buying new hardware. The consumer does not control the cloud infrastructure, but controls applications, operating systems, storage and some network features like firewalls. For example, if a clothing store needs additional computing power for its website during the holiday shopping season, it could buy cloud space from companies like Rackspace that provide direct access to cloud infrastructure without buying new hardware.[6] Similarly, NASA also rented computer power from Amazon to process information received from the Mars rovers.[7]
These three services are different from how the Internet was largely used at the turn of the century—and is often used today. In the recent past, users would often keep information on their own computers, rather than in an external location. For example, emails were often downloaded onto users' personal computers. Computer applications were also kept on a company or government agency's own computers, rather than on the servers of an external operator. Likewise, corporations that wanted more computing power during certain periods would simply buy more infrastructure, rather than contracting with a third party to temporarily buy more computing power.

**A. Benefits of Cloud Computing**

This new technology has a number of unique benefits, including its flexibility, improved customer service, improved security, and more efficient use of resources.

**Accessibility, Efficiency, Elasticity and Scalability**

Most obviously, cloud computing allows unprecedented access to information. Users can access data stored in the cloud from any computer or mobile phone with an Internet connection. Using Dropbox’s Software as a Service model, a user can save a spreadsheet or memo in New York that his colleagues in Dubai, Hong Kong and London can all access and edit instantly. The New York-based user can also protect these documents with a password, and may give access to as few or as many of his colleagues as he chooses.

Cloud computing allows customers to increase and decrease their computing capabilities rapidly. For example, companies like Rackspace provide Infrastructure as a Service to allow users to purchase electronic storage capacity immediately in any quantity at any time. Cloud computing also provides the greater potential for measured service, so cloud systems may offer the ability to optimize resource usage by measuring the exact resource use of each user and allocating accordingly. In such a way, resource usage can be more closely controlled and reported.

Cloud computing has also produced significant cost savings for users. A recent Brookings Institution study found that federal government agencies that migrated to the cloud for software and data storage saw between a 25 and 50 percent cost savings.[8] Cloud computing maximizes resource efficiency by eliminating the need to purchase additional hardware or software capacity to accommodate temporary upticks in usage.

Likewise, while personal computers are often used at levels far below their capacity, cloud computing allows companies or organizations in need (like the SETI at Home and NASA examples above) to take advantage of unused capacity. This reduces unused capacity, thereby preventing waste. Furthermore, since physical proximity to the user is unnecessary, cloud vendors may also choose to locate data centers where the energy costs associated with maintenance are lower. More efficient computing operations by cloud providers result in reduced energy usage and reduced costs for users.
Customer Service

Cloud computing allows users to access information and computing power in the cloud without any human interaction, which in turn reduces resources required for customer service. Built-in redundancies in the cloud reduce the probability of service outages for users. Moreover, cloud computing offers improved visibility of service usage—cloud computing providers can determine which features are most utilized and thereby target customer service and product development resources accordingly. Also, individual users may be able to reduce their IT staffs since customer service operations are often centralized in the cloud providers themselves.

Constant Security Updates

Cloud providers have complete control over their own security infrastructure, which allows them to update security measures without relying on users. These enhanced monitoring capabilities for providers and automated updates offer potential security benefits in the cloud. Thus, for example, someone using a word processor located on her computer rather than in the cloud (e.g. Microsoft Word) must download security updates and install them on her computer. This may lead to uneven security protections across networks. By contrast, the cloud provider and not the customer controls security updates for cloud-based word processing and spreadsheets services like GoogleDocs.

B. Security Challenges Posed by Cloud Computing

The same characteristics that make cloud computing so useful can also lead to significant security problems. As users are freed from the need to manage their computing infrastructure, they also lose control over security measures taken to protect their information and computing power. Many of these challenges also exist on non-cloud systems, but as data is aggregated in massive cloud vendors, it becomes a particularly tempting and lucrative target for hackers.

Potential Personnel Vulnerabilities

Information technology (IT) technicians with access to the cloud are usually unknown to cloud users. Many IT employees have direct access to information many cloud users would consider private, and can be responsible for designing and implementing security measures to protect that information. Like any industry responsible for storing and guarding sensitive information, cloud IT personnel may be points of vulnerability. In order to ensure data security, it is necessary to find IT personnel who are sophisticated, have strong qualifications, and who operate in a transparent manner. These employees have specialized education and training, and should be well compensated. This can be burdensome for emerging cloud computing companies, who may require long periods of time in order to become profitable and whose spending is often dependent on external fund-raising. As a result, cloud computing vendors sometimes lack qualified IT
personnel, and it is difficult for individual users to have much control over who protects or accesses their data or computing power.[9]

Data Loss

The interfaces of cloud computing software are also uniquely vulnerable. The actual log-in interfaces which are the gateway to accessing any cloud service must be highly encrypted, secure, and monitored. Interface security is necessary to prevent both data leakage, or accidental disclosure of data to insecure environments, as well as malicious entry. This issue applies across all forms of cloud computing—businesses, government, public users, and all other organizations are vulnerable to this issue so long as they utilize a cloud interface.[10]

One other area of concern is backup of data. As more people rely on the cloud for data storage, they may fail to back up their data elsewhere. If cloud data becomes compromised, sensitive user data may be corrupted or destroyed. Both cloud based and user controlled back up mechanisms provide additional data security and are particularly important for storage of sensitive data.

Third Party Programming

Part of the attractiveness of cloud computing is the scalability of the platform. Different parties can contract with each other to build upon an already established platform. However, each additional interface into a system provides more potential access and exploitation points into each cloud. Cloud providers must constantly update security measures pertaining to third party software and interface capabilities. This requires increased oversight from cloud providers and increasing cooperation between third party creators and cloud providers. When this oversight is lacking, security breaches can result.[11]

Difficulty of Determining Responsibility for Security Breaches

It can also be difficult to assign responsibility for security breaches. First, it may be simply unclear whether a security problem is coming from the cloud provider or the cloud user. Second, there are no clear rules as to whether the provider or the user is responsible for ensuring security. Cloud providers often are not transparent about how secure they are. As a result, users sometimes have little idea of the risk they are running by storing information with a cloud provider.[12]

Examples of Attacks on Information Stored in Cloud Servers

Given these vulnerabilities, it should be no surprise that there have been a number of high-profile attacks on information stored with cloud providers. For example in January 2010, Google announced that it had been hacked. The attack led to Google’s departure from China and a public dispute between the U.S. and Chinese governments.[13] Six months earlier, a hacker accessed Twitter’s financial documents and other business
information stored in a Twitter employee’s Google account.[14] Additionally, in May 2010, the Bureau of Engraving and Printing was hacked after the U.S. Department of the Treasury gave responsibility for hosting the website to a third party.[15] Most attacks on cloud servers are not reported, as companies are loathe to disclose potential vulnerabilities to the public, for a variety of reasons. Nevertheless, it is reasonably clear that hacks of cloud providers are increasingly common.

C. Other Drawbacks to Cloud Computing

In addition to security challenges, there are also practical and legal drawbacks to relying on cloud computing services.

Shutdown of the Cloud Computing Provider

As mentioned previously, many cloud providers are start-up companies. Customers relying on unproven cloud providers run a substantial risk that the provider will go out of business. In such a case, there is no guarantee that the customer will retain access to their cloud based data or be able to access applications they relied on in the cloud. Similarly, cloud users run the risk of losing their stored information and applications if they fail to pay their cloud providers.

Jurisdictional Problems

Almost any cloud computing system will implicate the laws of multiple jurisdictions. The laws of the users’ location, the location of the cloud provider or the location of an intermediary transmitting the information between user and provider may all potentially apply. The same data may be stored in multiple jurisdictions at the same time and the actual location of a user’s data may be difficult to determine or may be subject to change by the cloud provider without notice to the user. Although the application of the laws of multiple jurisdictions to a single cloud system is not itself an irresolvable conflict, some laws impose obligations regarding the storage or transmission of data which contradict the obligations imposed by other jurisdictions.

For example, many cloud computer providers are impacted by state requirements regarding the protection of financial or health information or destruction and disposal of consumer information.[16] As of February 2009, forty-five states, the District of Columbia, Puerto Rico and the Virgin Islands had enacted some form of a database breach notification act to protect personal information, in most cases only requiring disclosure to individuals whose data was compromised rather than particular security measures.[17] Some states have moved toward more stringent requirements. In 2008, both Nevada and Massachusetts created encryption requirements for the transmission of residents’ personal information.[18] State attorneys general are often empowered with powers to investigate unfair business practices similar to the powers available to the FTC that in practice allow them to prosecute privacy violations.[19] Cloud providers are often impacted by a number of these laws, depending on who their users are, where their data travels, and where their servers are located.
The same problem occurs with relation to foreign laws. Many cloud providers operate more or less without regard to national boundaries. However, different countries have differing levels of restrictions on how information can be shared. For example, the EU data protection directive often impacts cloud computing providers. The Directive specifically prohibits data transfers from EU members to countries with inadequate data protection laws, including the United States. In order to transfer data from the EU to the U.S., an entity must either adhere to the EU-U.S. “Safe Harbor” framework or rely on model contract clauses or binding corporate rules developed by the EU. The Safe Harbor framework was developed by the U.S. Department of Commerce and the EU Commission and is enforced by the FTC. The framework provides principles, such as notice, choice, access, and enforcement that an entity can adhere to in order to collect, store, process and disclose personal data about EU subjects in the U.S.

III. LEGAL ISSUES RAISED BY CLOUD COMPUTING RELEVANT TO NATIONAL SECURITY AND LAW ENFORCEMENT AGENTS

As the previous section has demonstrated, cloud computing is an increasingly important factor in modern communication. However, it also presents significant complications for law enforcement and national security officials in the U.S. First, as discussed in detail above, information stored in the cloud is a tempting target for hackers. Second, there are new challenges in collecting evidence that is stored in the cloud. Third, it can be difficult to present this information in court.

As a result, it is important to answer a number of questions, including: What laws protect users from crime in the cloud? How do law enforcement officers and other government agents cope with this innovation? How can they search and seize information stored on the cloud? This section will address these questions by exploring some of the legal issues associated with cloud computing. It will examine the following issues:

- What laws criminalize harmful activity in the cloud
- How government agents search and subpoena information on cloud networks
- What steps they must take in order to present this information in court

A. U.S. Laws Criminalizing Harmful Activity in the Cloud

Due to the novelty of cloud computing, there are only a few laws that regulate this method of storing and sharing information. Although states have their own computer crimes laws, the most important law regulating cloud computing is the federal Computer Fraud & Abuse Act (CFAA). While this law was not designed to target crime in the cloud—instead it was aimed at other kinds of criminal activity on computers—several of its provisions can be applied to harmful activity on the cloud.
The Computer Fraud & Abuse Act

Background to the CFAA

In the early 1980s, law enforcement agencies faced a lack of criminal laws available to fight emerging computer crimes.[21] Therefore, in the Comprehensive Crime Control Act of 1984, Congress enacted provisions to address the unauthorized access and use of computers and networks. In a new section focused entirely on computer crimes (18 U.S.C. § 1030) Congress made it a felony to access classified information on a computer without authorization, and a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer.[22] Congress conducted additional hearings and then enacted the Computer Fraud and Abuse Act in 1986, [23] which amended 18 U.S.C. § 1030 to reach a broader set of computer crimes, including intentional alteration or destruction of data belonging to others, theft of property via a computer in the context of a scheme to defraud, and trafficking in passwords and similar items. Since then, it has been amended several times as computer crimes have grown in sophistication, most prominently by the National Information Infrastructure Protection Act of 1996,[24] by the U.S.A. PATRIOT Act in 2001,[25] and by the Identity Theft Enforcement and Restitution Act in 2008.[26]

Today, the Computer Fraud and Abuse Act (CFAA) is one of the principal tools for combating computer crime. It currently prohibits seven different categories of crimes:

1. **Section 1030(a)(1):** This section prohibits obtaining or transmitting national security information from a computer. Penalties include up to ten years of prison. These crimes are considered a “Federal Crime of Terrorism” under 18 U.S.C. §2332(b)(g)(5)(B), which makes such crimes predicate offenses for prosecution under the Racketeer Influenced and Corrupt Organizations (RICO) statute.[27]

2. **Section 1030(a)(2):** This section prohibits intentionally gaining unauthorized access and obtaining information from a computer, even if no monetary damage is caused. This includes offenses such as hacking into banks to steal credit card numbers, hacking into a university to look at someone’s grades, or even hacking into Gmail to read someone’s email. This section protects all computers of government agencies and financial institutions. For other computers, it only protects those that have been compromised by an interstate or foreign communication. States must protect the confidentiality of computers from in-state intrusions. Penalties are typically a fine no more than $100,000 or up to a year of prison, unless certain aggravating factors apply, which can extend the fine to $250,000 and the prison sentence to five years. Examples of aggravating factors are that the offense was committed for commercial advantage or private financial gain, was committed in furtherance of a criminal or tortious act in violation of U.S. or state law, or the value of the information obtained exceeded $5,000.
3. **Section 1030(a)(3):** This section prohibits trespassing in a nonpublic government computer, even if no information is obtained nor any damage caused. Merely gaining unauthorized access to a government network may require the government to reconstitute its network, even if no other damage results. Violations are punishable by up to a year in prison for first-time offenders.

4. **Section 1030(a)(4):** This section prohibits using one’s unauthorized access to a protected computer in order to defraud and thereby obtain something of value. This overlaps considerably with the wire fraud statute.[28] Examples include hacking into a credit agency to alter one’s credit ratings so as to make purchases more cheaply,[29] using a lottery terminal to produce back-dated winning lottery tickets and collect prizes,[30] and stealing calling card numbers from a telephone company computer and then using those numbers to make free long-distance calls.[31] Penalties include up to five years in prison for first-time offenders.

5. **Section 1030(a)(5):** This section prohibits gaining unauthorized access and causing damage to a protected computer. This can include a broad range of activities, such as: hacking into databases to delete or alter records; transmitting viruses or worms that may delete files, crash computers, or install malicious software; or flooding a computer’s Internet connection with junk data, preventing legitimate users from sending or receiving anything with that computer, in what is known as a “denial of service” attack.

These crimes can cause many different types of damage, such as: preventing all Gmail users from accessing necessary emails for hours; crippling a business’s access to its inventory or customer data and thereby preventing sales or transactions; interfering with phone services such that emergency services cannot respond quickly to crimes, fires, or medical emergencies; or even disrupting traffic signals and causing car accidents. Installing malicious software without authorization, altering the security software on a computer so as to make unauthorized access easier later, or defacing a website can constitute damage as well.[32] Penalties vary based upon the mental states of the intruder, ranging from one year to ten years imprisonment for first-time offenders.

To prove a violation of this provision, the statute requires proof of at least one of the following enumerated types of harm: at least $5000 of economic loss in any one-year period, an effect on medical care, physical injury to a person, a threat to public health or safety, or damage to a computer used in the administration of justice or national security.[33] The most commonly charged crime is economic loss, which is broadly defined as “any reasonable cost” including response costs, costs of restoring computer systems, and lost revenue or other consequential damages.[34] The $5000 threshold may be met by aggregating all the losses of all the victims of a particular intruder that occur within a one-year period. However, the extent of damages may still be difficult to prove in some cases. While a company can calculate the salary and equipment costs of responding to an attack,
this is considerably more difficult for an individual, who may spend many frustrated hours but little money.

6. **Section 1030(a)(6):** This section prohibits trafficking in passwords or similar information that could be used to gain unauthorized access to a protected computer.

7. **Section 1030(a)(7):** This section prohibits threatening to cause damage to a protected computer with the intent to extort. Criminals frequently threaten to use their unauthorized access to destroy sensitive data or cripple important computer infrastructure. For example, a computer security expert who hears rumors of impending layoffs may write malicious code into his employer’s computer system, which would allow him to effectively hold the computer system hostage so as to ensure his continued employment. Penalties for first offenses can reach up to five years in prison.

It is important to recognize that many of the offenses in the CFAA require that the intruder either access a computer “without authorization” or otherwise “exceed authorized access.”[35] Persons who exceed authorized access are likely to be insiders, whereas those who act without authorization are likely to be outsiders. Insiders, who already have some access, generally face criminal liability only if they intend to cause damage, whereas outsiders who break into a computer are generally also liable for reckless or other damage.[36] This reflects the difference between, for example, an IRS employee who exceeds his authorized access by looking at tax records for personal purposes, [37] and a hacker who breaks into a company’s customer databases without authorization.[38] Cases that involve exceeding authorized access require determining the precise scope of the user’s authorization, which can turn on documents such as employee confidentiality agreements,[39] or terms of service agreements for websites.[40]

Further, in addition to subjecting offenders to federal prosecution, the CFAA also authorizes civil actions for compensatory damages and equitable relief.[41] However, civil actions are only available if the offense causes a physical injury, a threat to public health or safety, interference with medical care, interference with government computers used for administering justice or national security, or at least $5000 of aggregate damage within a one-year period.[42] Civil actions must also be brought within two years of the discovery of the damage.

*Application to Cloud Computing*

There is no question that the CFAA applies to cloud providers. The Act covers “protected computers,” which is defined as any computer used in or affecting interstate or foreign commerce, as well as any computer of the federal government or a financial institution.[43] This includes any computer connected to the Internet, even if outside the United States. Thus, servers anywhere in the world that host cloud computing services or resources can be protected by the Act.
In addition, several provisions of the CFAA can be used to punish harmful activity in the cloud:

- **Section 1030(a)(2):** As mentioned above, this provision criminalizes unauthorized access to a protected computer. This provision was originally intended to protect the privacy of individuals by criminalizing unauthorized access to credit records or other computerized information. As such, it seems especially appropriate for protecting information in the cloud from unauthorized access, as long as that access is provably from across state lines.

However, individuals frequently do not know if their information has been accessed without authorization or even where their information is stored. Furthermore, prosecutors typically have difficulty establishing the aggravating factors under the statute that trigger felony penalties, and this difficulty is amplified in the context of the cloud. If a hacker illegally accesses a cloud datacenter and obtains information worth $20 each from 1,000 or more different accounts, a prosecutor may need to gather information from the owners of hundreds of accounts before being able to prove that the value of the information obtained exceeded $5,000. Furthermore, despite having accessed the information of thousands of users via a single illegal entry, such a hacker would only face the same maximum penalty as if he had hacked into a single PC.

- **Section 1030(a)(5):** As described above, this section criminalizes damage to a protected computer. As a result, it protects cloud providers who suffer damage as a result of a malicious attacker, provided the attack comes across interstate lines.

However, the section is not always applicable. In particular, if someone attacks a cloud datacenter and causes a very small amount of damage to each of a very large number of people, it may be very difficult for law enforcement to calculate precisely how much damage each individual has suffered without detailed investigations of the accounts of thousands of people. These challenges are similar to those faced by prosecutors attempting to establish the aggravating factors in Section 1030(a)(2).

- **Section 1030(a)(6):** As described above, this prohibits trafficking in passwords or other tools used to gain unauthorized access to a protected computer. Because cloud datacenters are generally protected computers, passwords or login information that customers use to access cloud services are protected by this provision. Penalties include one year of prison for first-time offenders.

- **Civil Damages:** As mentioned above, the CFAA allows private actors to pursue civil claims against actors who cause more than $5,000 worth of damages in a single year, which also could covers attacks on cloud providers. This can help to prevent cyber crime on cloud networks.

However, currently civil actions can only be brought by those who suffer the damage themselves, and so cannot be brought by cloud service providers on behalf of their
customers. Attacks on cloud data centers can be very lucrative if they affect a very large number of customers, but affect each one to only a minor degree. Furthermore, even trained customers will rarely be able to identify their attackers, since the attacks take place not against the customers’ computers, but against cloud datacenters owned and managed by various cloud service providers. It is likely that in many circumstances, no single user will have the incentive or ability to bring a civil suit in response to an attack on cloud infrastructure. As such, in many cases only cloud service providers have the incentives and the information necessary to bring viable civil claims and thereby serve as an effective deterrent against cybercrime.

B. Searching & Seizing Information on Cloud Computing Networks

Obviously, government agents have a strong interest in being able to search and seize information stored on cloud computer networks. Government agents may wish to do so in order to punish e-crime against cloud providers, or in order to punish other sorts of crime. For example, child pornography rings have operated off cloud providers such as Facebook.[45] There are three methods by which government agents might receive this information: get the information under the Electronic Communications Privacy Act, get an ordinary warrant, or ask for a FISA warrant.

The Electronic Communications Privacy Act

Passed in 1986, the Electronic Communications Privacy Act (ECPA) sought to “bring the constitutional and statutory protections against wiretapping of telephonic communications into the computer age.”[46] ECPA was written at a time when network computing was used for two primary purposes. First, network account holders would use third-party network service providers to send and receive communications, having the providers hold the messages until delivery to the user’s computer. Second, account holders used third-parties to outsource computing tasks such as storing and processing large amounts of data.[47] At that time, “very few Americans had e-mail accounts, and those who did typically downloaded email from a server onto their hard drives, and email was automatically and regularly overwritten by service providers grappling with storage constraints.”[48]

The part of ECPA that covers searches and seizures on an electronic network is called the “Stored Communications Act” (SCA). The SCA froze into law the two understandings of network computer use described above. According to the SCA, there are two types of network providers: electronic communication service (“ECS”) and remote computing service (“RCS”). An ECS is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”[49] “Electronic storage” is “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” and “any storage of such communication by an [ECS] for purposes of backup protection of such communication.”[50] An RCS is defined as “the provision to the public of computer storage or processing services by means of electronic communication service.”[51]
ECPA did not foresee the proliferation of cloud-based storage systems that allow individuals and business to retain all their emails or free up their storage space by placing data on trusted third-party servers. This data includes highly personal information such as financial data, medical records, and intimate correspondence. If such materials were stored on one’s hard-drive, CD, or in a safe deposit box, law enforcement agents would have to apply for an ordinary warrant. But under ECPA, a single email or document could be subject to multiple legal standards throughout its lifecycle. A communication can fall into one of three categories, each with different privacy protections:

- Communication held by an ECS in “electronic storage” for less than 181 days: For these types of communications, the government can compel the provider to disclose information to the government only through an ordinary search warrant pursuant to the Fourth Amendment.

- Communication held by an ECS in “electronic storage” for 181 days or more: For these types of communications, the government can compel the disclosure of information through a warrant, but also an administrative subpoena, or court order. Subpoenas are much easier to obtain: they do not require a showing of probable cause, but instead a showing that the requested materials are evidentiary or relevant. Additionally, while a judge always reviews an application for a warrant, subpoenas may be issued by attorneys or court clerks. Further, the government may delay notification to the individual whose communications are being monitored for up to ninety days.

- Communications held by an RCS can be compelled through a warrant, administrative subpoena, or court order, regardless of duration of storage.

Therefore, there are two crucial issues when government agents want to search for information in the cloud: (1) what counts as “electronic storage” and, (2) the scope of ECS versus RCS.

In terms of “electronic storage,” what is undisputedly included are communications held by a service provider and not yet retrieved by a subscriber, such as an unopened email. But beyond that is not clear. ECPA did not foresee web-based email clients such as Gmail, where users leave all email—unopened and opened—on Google’s servers. Are such messages “electronic storage”? The Department of Justice’s (DOJ) manual on searching and seizing electronic evidence does not believe so, holding that “electronic storage” only covers unopened email messages. DOJ contends that once the email is retrieved by the recipient it is no longer in “temporary, intermediate storage . . . incidental to . . . electronic transmission.” There is support for this view in the legislative history of EPCA.

The Ninth Circuit rejected this narrow interpretation in Theofel v. Farey-Jones. The court found that while opened messages do not fall within the first prong of the
“electronic storage” definition, they do fit comfortably within subsection (B): the storage of electronic communications for purposes of backup protection.[62]

But the Theofel court was operating under the assumption that users download emails to their computers, therefore making the copy that remains on the remote server necessarily a backup. This is not the case in a cloud computing system, where the remote server may be the only place the user stores their documents. The U.S. District Court for the Central District of Illinois recognized this distinction in United States v. Weaver.[63] The Weaver court was faced with the issue of whether Hotmail, a web-based email provider, should be classified as an ECS or RCS. The court found that Hotmail was an RCS, because users store their messages on Hotmail’s remote system. Hotmail, therefore, is maintaining the messages “solely for the purpose of providing storage or computer processing services to such subscriber or customer.”[64] Thus, a trial subpoena is sufficient to compel production of the communications.

The introduction of Internet-based applications beyond email further complicates the issues. ECPA may provide a relatively clear answer for email, which is intended to be a communication between parties. What is much more difficult is how to treat something like a document on Google Docs: a word processing document that the user may have no intention to communicate with anyone, but instead wants to store in the cloud to free up space on his personal machine and/or allow him to access the document from any computer. While many in the industry claim otherwise, the Department of Justice has argued that ECPA is actually well suited to address such matters because storing such files in the “cloud” is a similar situation to the one ECPA was born into. In 1986, most data storage was offsite. As personal computers gained storage capacity, remote storage became less popular, but now the pendulum has swung back toward more outsourced storage. Seen in this light, the application of EPCA is obvious: “The law is pretty clear that storage services qualify as remote computing services [“RCS”] under Section 2703(b),” said Richard Downing, an attorney with DOJ’s computer crimes and intellectual property section.[65] Under this view, much of the information that the average user would assume is protected by the Fourth Amendment is in fact accessible to the government by merely obtaining a court order or administrative subpoena.

Google disagrees, claiming that cloud computing is an ECS, requiring law enforcement to obtain a warrant.[66] Digital Due Process, a coalition with members as diverse as the ACLU, Microsoft, and Americans for Tax Reform have called for ECPA reform, characterizing the current law as a “patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies.”[67]

The Fourth Amendment

On its face, therefore, ECPA sometimes allows law enforcement officials to get information from cloud providers without obtaining an ordinary warrant. However, it is possible that searches of information stored on the cloud are protected by the Fourth Amendment. If so, law enforcement officials would need an ordinary warrant to search
information stored on the cloud. Regardless of what ECPA says, what kinds of data are protected by the Fourth Amendment, and require a warrant to search?

**Background to the Fourth Amendment**

Whether the Fourth Amendment applies, and thus whether a subpoena or warrant is necessary, depends in large measure on whether the owner of the information had a reasonable expectation of privacy. The Fourth Amendment will apply, and a subpoena or warrant will be required if the owner actually believed the information would remain private, as demonstrated by his efforts to conceal the information, and if that belief was reasonable according to prevailing public expectations of privacy. Thus, taking private information into the public sphere does not destroy the privacy interest (and end Fourth Amendment protections), if it is concealed. For example, taking private documents into a busy street does not destroy the privacy interest if the documents are stored in something like a briefcase. That protection is lost, however, if someone purposefully encourages the public to access the information, or makes no attempt to conceal it from the public. The Fourth Amendment privacy analysis has adapted to both the computer itself and the separate sections of hard drives known as “platters,” with courts recognizing both as discrete containers each requiring its own justification for a government search. Courts have also recognized various levels of data storage (e.g. folders, files) as individual “virtual containers” within the larger container of the hard drive. They have also accepted password protection as a sufficient concealment measure to satisfy the Fourth Amendment requirement.

**The Fourth Amendment and the Cloud**

The cloud complicates matters because third parties have unprecedented access to communications that were considered private in previous media. In Fourth Amendment analysis, information voluntarily given to a third party business under the “third party doctrine” does not always remain private. For example, phone customers cannot retain a reasonable expectation of privacy in non-content subscriber or transactional data that phone companies collect in the regular course of business. This transactional data includes basic information like the phone numbers of the callers, as well as the time and length of the calls; it also applies to bank, tax and other business records. Likewise, federal courts have uniformly held that an Internet Service Provider’s (ISP) transactional information (e.g. IP address and time logged on) is not protected by the Fourth Amendment under the third party doctrine. However, a user’s content may retain a privacy interest though placed with a third party for “safekeeping.” This could mean that the content of text messages and emails held remotely are protected by the Fourth Amendment and thus require a warrant or subpoena for government access. However, cloud service providers employ user content in ways that other communications service providers do not, making for a much more complicated, and as yet unanswered question.

Taking a site like Facebook as an example may illuminate the issue. Social networking sites like Facebook allow users to share files in multiple formats and send and receive
messages using a password-protected account. Though a public forum, Facebook privacy controls allow a user to customize who may access her data, which she may make fully public (i.e. available to anyone on the Internet, even non-Facebook users) or limit to “friends” (Facebook subscribers who a user has accepted into her social network). A user may further limit access to her files by blocking certain friends from viewing certain kinds of data. Conceivably, a user could block all of her friends from viewing her data, or may save drafts of text without transmitting them to anyone, thus using Facebook like a cloud-based data storage unit.[84] Facebook is a public forum, but it houses objects that courts have categorized as “highly personal items [such] as photographs, letters, and diaries”[85] which are presumptively private unless shared with the public. As discussed previously, placing private objects or information in a public place does not automatically destroy its privacy interest if efforts to conceal it remain, as in a container.[86] Clearly, if a Facebook user chooses to share some of her files with the public, those files have no Fourth Amendment protection. If she shares other files with a single person while storing others out of sight, she may be able to preserve Fourth Amendment protections in both, though assuming the risk that those files that she has shared with the other person may lose Fourth Amendment protections if the other person exposes them publicly.

Then the question arises: if the government sought to search the Facebook user’s non-public information, what exactly is it searching—i.e. what should it consider the “container” in defining the scope of its warrant? Is the entire Facebook account a single “virtual container,” which the user’s password makes opaque/concealed, thus only requiring law enforcement to obtain a single warrant to search the entire account? Or do the privacy controls mimic separate virtual containers and thus law enforcement must justify access to each kind of data separately, despite the fact that the data may not be stored in separate online “folders”? Or does the “container” also depend on the structure of the hosting site’s servers as it did in cases where files were contained on a user’s home computer? Even if a court were to resolve these questions, another more fundamental one remains—can any data in the cloud retain Fourth Amendment protections in the face of the third party doctrine? This will likely depend on what courts ultimately determine to be sufficient concealment efforts. Is a password sufficient to conceal and thus protect privacy interest in an object?[87] Is a deliberately obscure web address, as in “unlisted” websites, combined with an authentication key a sufficient effort at concealment to ensure Fourth Amendment protection?[88]

The issue of whether third party access to information destroys the user’s privacy interest becomes more complicated for many of the most popular cloud providers that use user data more liberally, like Gmail. For example, Google accesses user search queries and message content to offer tailored advertising. In so doing, these cloud providers collect much more content-based information than their telephone or even ISP counterparts, going far beyond the “transactional” data including date, time, origin and destination of a call or message.[89] Similarly, Netflix, the web-based DVD rental agency, utilizes viewing patterns to supply custom DVD recommendations, and Amazon uses purchasing patterns to recommend other items for purchase. One federal appeals court has held that a Fourth Amendment privacy interest may remain despite some third party email scanning, as when an ISP scans for viruses and prohibited material (like child
pornography), analogizing the scan to the postal service’s screening of packages for drugs and explosives. However, cloud providers’ use of user content has become much more invasive and more entangled than these scans, as it interacts with the user by providing new recommendations, thereby providing constant reminders that the user is not its only viewer. Nonetheless, this analogy may prove useful where the third party doctrine would otherwise destroy all private interest in data that users increasingly depend upon and may commonly view as private, despite their legal status.

It is difficult to see how a privacy interest could survive such regular, invasive usage of user data without a significant expansion of exceptions to the third party doctrine. Fourth Amendment protection for cloud data will also depend on how user agreements allow cloud service providers to utilize user content. There is some indication that courts would find a privacy interest survived where service provider agreements do not provide for regular content monitoring. Thus, a great deal of power will likely continue to rest with cloud service providers to determine the boundaries of user privacy and government access to information, absent legislation or significant changes in judicial interpretation of the third party doctrine.

Reasonableness of Scope for Subpoenas and Searches

As in the analysis above regarding what qualifies as a search, the reasonableness analysis for both subpoenas and warrants depends in great measure on a court’s definition of container, as it delineates the proper bounds of a reasonable search or subpoena. (Returning to the Facebook example, a finding that the password provided opacity for the account as a single container, the subpoena or warrant’s reach would be considerably greater than if each individual privacy control established its own container.) The Supreme Court recently held that violations of other statutes that govern standards for warrants, like the Stored Communications Act, do not necessarily make a search per se unreasonable.

The Foreign Intelligence Surveillance Act

In addition to ordinary search warrants or subpoenas, U.S. government agents may also apply under the Foreign Intelligence Surveillance Act (FISA) for FISA warrants. FISA warrants must be focused on gathering foreign intelligence, where domestic sources encountered are only incidental to the intended focus of the warrant. Cloud computing may complicate the FISA warrant process, as content that originates with a foreign source may ultimately be stored domestically, or vice versa, and data may traverse a number of other domestic or foreign servers en route to and from its destination. Specifically, FISA after the FISA Amendments Act differentiates between whether surveillance is being conducted inside or outside the United States. The geographical fuzziness that accompanies cloud computing may make drawing this distinction difficult.

Furthermore, foreign governments and companies may try to avoid using cloud providers with U.S. storage facilities in order to avoid the reach of U.S. intelligence-gathering procedures like FISA, as well as the PATRIOT Act and National Security Letters.
National Security Letters are administrative subpoenas used by federal agencies involved in foreign intelligence gathering that request customer information from communications providers, financial institutions, and other third parties. The Letters contain nondisclosures requirements that prevent the recipient from revealing their receipt of a Letter or its contents, including to the subject whose information is being collected. Many commercial cloud providers, such as Microsoft and Google, are potentially subject to such requests, which can be a concern for potential non-U.S. customers. The Canadian government, for example, has a policy of refusing to use U.S.-based hosting services for public sector IT projects.

C. Presenting Information from the Cloud in Court

The final issue faced by law enforcement and national security officials in this area is presenting information stored by the cloud in court. There are two hurdles to overcome: the practical issue of how easy it is to search for information stored in the cloud, and the difficulty of satisfying the chain of evidence requirements demanded by courts.

Accessibility of information stored in the Cloud

The accessibility of cloud data to law enforcement depends upon service provider practices (i.e. how long they retain copies of files, whether signatures of files a user deletes still remain, etc.), which may in turn be determined by their potential liability under statutory regimes. Access may also be limited by encryption practices of both users and providers. As more user-operated encryption devices become available, law enforcement access to cloud data may become more difficult. However, many users continue to rely on service-based encryption, which may allow government access through cooperative agreements with cloud operators.

Forensic/Chain of Custody Concerns

Cloud computing raises a number of unique forensic issues, including the location of potential digital evidence, its preservation, and the subsequent forensic analysis.

In order to prove a piece of evidence’s authenticity and absence of tampering, a chain of custody is maintained. In the case of a tangible item—such as a knife—the item is carefully gathered, bagged, tagged, tested and kept safe in an evidence room until trial. Every time the item changes hands, a log is updated. But when electronic information needs to be maintained, the chain of custody becomes two-dimensional—both tangible and intangible objects need to be tracked and preserved. Therefore, when applying a chain of custody to digital evidence, not only must the law enforcement agency track the physical storage item (i.e. hard drive), but also the intangible documents and e-mails stored on that physical item.

Traditionally, when a law enforcement agency desires to investigate digital files, they can seize the physical equipment the data is stored on. By essentially freezing the
information, the likelihood of the data being removed, overwritten, deleted or destroyed by the perpetrator is low, increasing the probability that the data will be admissible evidence. But investigating in the cloud is more difficult, because data for multiple customers may be located on the same server, or alternatively, spread across an ever-changing set of hosts and data centers.

If a person uses an application in the cloud, registry entries (which record user activity) and temporary files will be stored in the virtual environment. When the user exits the application, those files in the virtual environment will be lost, making evidence traditionally stored on the computer’s hard drive potentially unrecoverable.

Current forensic technologies do not consider or understand the concept of multiple tenants on an environment. They assume the “one tenant, one physical host” construct. So when presented with multiple tenants in a cloud environment, it is possible that data will be acquired from tenants not under investigation. This problem was illustrated by a case from spring 2009. Core IP Networks leased facilities to the owners of data servers, including a cloud computing service provider named Liquid Motors (LM). LM helps auto dealers manage their inventory and Internet marketing. After accumulating evidence that a criminal enterprise had used LM’s servers or some of the data stored in those servers to further its criminal activity, the FBI obtained a search warrant to seize control of the servers. There was no accusation of wrongdoing by LM, but the seizure shut down LM and debilitated the operations of their innocent customers. LM went to court, requesting the FBI release the servers, claiming they and their customers were suffering great economic harm. The court denied the request, finding that the FBI had adequate justification to hold the servers. Though the FBI was allowed to hold the servers, the prosecutor still faces challenges. If data on cloud servers is shared, it will be very difficult for prosecutors to ensure the data retrieved and presented are artifacts of evidential value that are complete, accurate, and verifiable, thus opening the door for reasonable doubt.

To address this problem, Benjamin Wright, a computer forensics expert, recommends that companies “spread or duplicate their data and services across multiple service providers, located in multiple jurisdictions.” But this presents a host of problems for government investigators and prosecutors. First, while there are tools available to collect data in the cloud, not all cloud providers have such systems as the default. Therefore, those users not willing to pay for the added forensic tools will find it much more difficult to recover data should it become necessary.

Second, the ability of data sent to the cloud to be stored anywhere in the world—including countries where privacy laws are not readily enforced or non-existent—creates problems. Gathering evidence stored in foreign countries can involve each nation’s diplomatic actors, adding delays and costs to the investigation. Where the burden of proof lies with the prosecution, it will be difficult for the prosecution to prove “beyond a reasonable doubt that cross-contamination of evidential data has not occurred.”
IV. RECOMMENDATIONS

A. Simplify the Electronic Communications Privacy Act

As discussed in Section III.A, the Electronic Communications Privacy Act (ECPA) governs the collection of electronic data. As individuals and businesses rely on technology to a greater extent, “ECPA now define[s] a crucial bulwark of privacy in modern life.”[108] But ECPA’s standards are needlessly complicated and its protections are strikingly limited given the increasing use of cloud computing technology.[109]

A sensible revision to ECPA would require law enforcement to demonstrate probable cause consistent with the Fourth Amendment when seeking the content of electronic communications. Such a change would greatly simplify the current standard, where the requirements for law enforcement turn on the type of service provider storing the data and the length of the storage. Changing ECPA to a single standard has two principal benefits. First, a simplified standard will reduce law enforcement confusion concerning what procedures need to be followed. For example, if law enforcement desires the contents of an email, in order to determine whether it must obtain a warrant or can proceed with a subpoena or court order, law enforcement must determine whether the email (1) has been opened or unopened; (2) is in transit or at its final destination; (3) is stored on an ECS or an RCS; and (4) is older than 180 days. And even then, courts are confused as to what is required of law enforcement. Dispensing with this multi-factor test will result in more predictability and stability in government investigations. Importantly, this would not upset the lower burden on the government when it seeks non-content information from electronic communications. To intercept non-content information such as the recipient of an email, the time it was sent, or its size, only an administrative subpoena is required by the government.[110]

Second, raising the standard to probable cause will better comport with the public’s expectations of the privacy afforded to their online data. When ECPA was passed in 1986, computers were still in their infancy. Nearly 25 years later, we have come to rely on computers in ways never imagined. For many, computers are now used as the primary means of personal correspondence and as a repository for medical and financial information. Given our reliance on computer technology, it might be shocking for computer users to learn that, for instance, the Department of Justice and several federal district courts believe that email stored in a cloud service is in a “Remote Computing Service” and therefore can be obtained with as little as an administrative subpoena. Society has taken data out of the privacy of safety deposit boxes and sealed envelopes and placed it in the “cloud” for efficiency, cost, and flexibility. ECPA should recognize this new reality and provide the same privacy protections to these new storage mechanisms as to their physical counterparts.
B. Amend the Computer Fraud and Abuse Act to Allow Prosecutions Based on Number of Users Affected or Amount of Information Taken

Section 1030(a)(5) of the CFAA prohibits gaining unauthorized access and causing at least $5000 of economic loss in any one-year period to a protected computer or computers. Similarly, Section 1030(a)(2) prohibits intentionally gaining unauthorized access and obtaining information from a computer, even if no monetary damage is caused, but increases the penalties if the value of the information obtained exceeds $5000. These sections of the CFAA can be used to prosecute malicious users who obtain unauthorized access to information stored in the cloud such as credit card information, or who attack cloud service providers themselves. But the government’s task in proving the damage caused exceeds $5000 is unnecessarily complicated if the attack affected a large number of users but only caused nominal damage to each. For example, if the attack caused $20 of damage to all users, the prosecutor would need to gather information from hundreds of accounts before being able to clear the $5000 threshold.

Instead of forcing prosecutors to undertake such an arduous task, the CFAA should be amended to allow prosecutions based on the numbers of users whose information is stolen or the amount of total information taken. This will facilitate prosecutions as the government would not need to conduct thousands of detailed individual investigations in order to determine the value of each user’s stolen data. Consequently, these prosecutions more closely resemble those for an attack on a single computer, presumably the scenario the original drafters had in mind.

Additionally, Section 1030(g) permits victims to seek compensatory damages if the value of the damage caused within a one-year period exceeds $5000. A civil action can only be brought by those who suffer damages themselves, and so cannot be brought by cloud service providers on behalf of their customers. Similar to the problem discussed above, there could be a scenario where a user attacks a provider, gaining unauthorized access to a small amount of data from a large number of users. Though the attacker has stolen well over $5000 worth of data, each individual has only lost a nominal amount. Therefore, it is likely in many circumstances that no single user will have the incentive to bring a civil suit, thereby eliminating a tool to combat cyber crime on cloud networks.

To better harmonize Section 1030(g)’s goals with the characteristics of cloud computing, the section should be amended to allow cloud service providers to bring civil actions on behalf of their clients, and/or allow a group of affected users to form a class and bring a class action against the attacker. This would lower transaction costs, making it more likely that victims would seek to vindicate their right to damages following an attack in the cloud.

C. Require All Cloud Service Providers to Have the Technology to Give Them the Ability to Collect Data in the Cloud if Needed for a Government Investigation
Section III.C detailed the criminal forensic issues presented by cloud computing, including the necessity of relying on cloud service providers to preserve information that may be useful or necessary to a government investigation. As detailed above, some cloud service providers’ default service does not include the tools necessary to collect data in the cloud, offering such tools to customers only for an additional charge. Those users hoping to maximize the cost savings presented by cloud computing may forgo such add-ons. But if those users’ information should be needed in connection with a government investigation, agents may be frustrated to learn that the data has not been properly preserved. Therefore, Congress should enact legislation requiring all cloud service providers to provide, at a minimum, the tools necessary to preserve data stored in the cloud.

[4] Id.
[11] Id. at 37.
[12] Id. at 28.


[19] 201 Mass. Code Regs. § 17.00 (2008) (requiring encryption of personal information while transmitted over a public network or wirelessly); Nev. Rev. Stat. § 597.970 (requiring encryption of personal information being transmitted outside of the secure system of the business)


[35] § 1030(e)(11).

[36] § 1030(e)(6).


[38] United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997).


[40] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).


[44] § 1030(e)(2).


Id. §§ 2703(a)-(b).

Id. § 2705(a).

Id. § 2703(b).


See H.R. Rep. No. 99-647, at 65 (1986) (stating that when a recipient has retrieved an email message and chooses to leave it in storage with the service provider, the email is protected under a provision of 18 U.S.C. § 2702 applicable to remote computing services).

359 F.2d 1066 (9th Cir. 2004).

Id. at 1075.


Id. at 772 (citing 18 U.S.C. § 2703(b)(2)).


Not all government action qualifies as a search with Fourth Amendment protections—a search only occurs when the government attempts to search an object or information in which the owner had a reasonable expectation of privacy. Katz v. United States, 389 U.S. 347, 360-61 (1967).
[71] United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

[72] U.S. v. Perrine, 518 F.3d 1196, 1207 (10th Cir. 2008)(holding that connection to peer-to-peer file sharing network allowing all Internet users to access files destroyed any reasonable expectation of privacy).

[73] See e.g. United States v. Andrus, 483 F.3d 711, 719-22 (10th Cir. 2007).


[76] See e.g. United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005) (reasonable concealment measures necessary to justify expectation of privacy).


[78] Id.


[80] Perrine, 518 F.3d at 1204 (citing line of cases supporting this proposition). Access to other “transactional data” may be more controversial—unlike telephones, email addresses are usually dedicated to a single person, making it much easier for a company or government searcher to determine who used the account at a particular time when compared to pen register information.

[81] United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983)(holding that unlocked briefcase entrusted to third party retained Fourth Amendment protections).


[83] Warshak, 490 F.3d at 475.

[84] However, the question remains open, with courts providing little guidance on the contours of the Fourth Amendment for remotely held digital data generally, and none whatsoever regarding the specific challenges of the cloud. Warshak, the case regarding ISP access to a user’s emails, was vacated on other grounds. In Quon, the Ninth Circuit held that a government employee user of a government-provided pager retained a reasonable expectation of privacy in text messages held remotely by a service provider. On appeal, the Supreme Court chose to decide the issue on narrower grounds, overturning the Ninth Circuit’s holding regarding the search’s reasonableness, while assuming without deciding the issue of reasonable expectation of privacy in the text message.

[85] Similarly, some blogging sites have security controls that allow a user to use a single password protected account to set a variety of public access levels from public to completely private, for information they place in the cloud.


[87] United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

[88] Outside the cloud context, courts have been divided on whether password protection was sufficient to preserve a user’s privacy interest in protected files on a shared
computer. DEFOGGING at 2224, citing Trulock v. Freeh, 275 F.3d 391, 398, 403 (4th Cir. 2001) (holding that girlfriend could not consent to search of boyfriend's password-protected files on shared computer); but see United States v. Andrus, 483 F.3d 711, 719-22 (10th Cir. 2007) (father could consent to police search of son’s password-protected files; password insufficient to preserve privacy interest).

[89] Unlisted websites have highly specific/complex web addresses designed to prevent access by all but authorized users who know the exact address of the site. For more discussion see DEFOGGING at 2235-56.


[91] Warshak, 490 F.3d at 474.

[92] Id.


[97] DEFOGGING at 2217.


[101] Id.

[102] Frowen, supra note 2.


[105] Id.

[106] Id.


[110] See Part III.B


[113] Id. §1030(a)(2).