THE IMPLICATIONS OF THE ABANDONED PROPERTY DOCTRINE OF THE FOURTH AMENDMENT ON DATA DELETED FROM THE CLOUD

By

William C Pizio

Capstone Project Submitted to the Faculty of

Utica College

April, 2013

In Partial Fulfillment of the Requirements for the Degree of Master of Science of

Cybersecurity
ABSTRACT

Under current law, cloud data enjoys a lesser expectation of privacy compared to locally stored data and deleted cloud data may enjoy no Constitutional protections at all. While law enforcement access to locally stored data requires a search warrant, cloud data can require as little as a court order or subpoena to gain access, and there is little legislative or judicial guidance as to the protections afforded to deleted cloud data. With the Electronic Communications Privacy Act of 1986 in need of updating and the rise in emerging technology issues in criminal appellate cases, a better understanding of the role of deleted cloud data as evidence in criminal prosecutions is necessary. Using the Katz reasonable expectation of privacy test and the abandoned property doctrine, this research concluded that deleted cloud data should enjoy the full protections of the Fourth Amendment. By separating cloud data from the third party doctrine and by differentiating between disposal and permanent deletion, users who choose to make their data permanently inaccessible exemplifies the intent to keep the data private, thereby maintaining their Fourth Amendment protections. Keywords: Cybersecurity, Christopher Riddell, ECS, RCS.
# TABLE OF CONTENTS

The Implications of the Abandoned Property Doctrine of the Fourth Amendment on Data Deleted from the Cloud.................................................................1  
**Literature Review**.........................................................................................3  
  - The Fourth Amendment and the Expectation of Privacy............................3  
  - Introduction to the Fourth Amendment......................................................3  
  - Evolution of the expectation of privacy.....................................................4  
  - The third party doctrine and the expectation of privacy............................6  
  - The abandonment doctrine and the expectation of privacy.........................7  
**Digital Technology: Statutory and Constitutional Protections**.........................9  
  - Electronic Communications Privacy Act of 1986......................................10  
  - Existing judicial precedents......................................................................12  
  - Cloud Computing.....................................................................................13  
  - The cloud and subscriber privacy............................................................14  
  - Data deleted from the cloud......................................................................16  
**Summary**.....................................................................................................17  
**Discussion of the Findings**........................................................................18  
  - Fourth Amendment Protections for Data Stored in the Cloud....................18  
  - Fourth Amendment Protections for Data Deleted from the Cloud..............21  
**Recommendations**......................................................................................25  
    ................................................................................................................25  
  - Cloud data as RCS.................................................................................25  
  - Search warrants to gain access to cloud data..........................................25  
  - ECPA protections for deleted cloud data .................................................26  
  - Cloud Storage Provider Duty: Deletion Should Equal Deletion................27  
  - Fourth Amendment Protections for Deleted Cloud Data............................27  
  - Judicial Education and Training...............................................................28  
  - Further Research.....................................................................................29  
**Conclusions**...............................................................................................30  
**References**.................................................................................................32
The Implications of the Abandoned Property Doctrine of the Fourth Amendment on Data Deleted from the Cloud

In the last five years, cloud computing has become one of the most transformative developments in the history of computers and computing. It has begun to significantly change the way information technology is created, delivered, accessed, and managed (Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M., 2011a) and according to Gartner (2009), annual revenue for cloud providers has grown substantially and is expected to reach $150 billion in 2013. At the end of 2012, the estimated number of worldwide active Yahoo! Mail, Gmail, and Hotmail users was reported to be between 750 million and 1 billion users (Brownlow, 2012). The Pew Research Center also reported that approximately 69% of online Americans utilize cloud services that includes webmail services, storing personal photos or videos online (i.e. Facebook), using online applications such as Google Drive, storing computer files online, or backing up a hard drive to an online site (Horrigan, 2008). In all, there is little evidence to suggest that the number of cloud service users will not continue to increase.

With computers being utilized for criminal purposes, there is an increasing use of digital information revealed via computer forensics in criminal investigations by law enforcement. For those individuals who are heavy cloud users, there may be little digital evidence on machines that the specific individual or investigator has access to (Horrigan 2008). Data stored on a local machine is deemed the same as other tangible property of a suspect and is clearly protected by the Fourth Amendment (Crowther, 2012). Data stored in the cloud differs from data stored on a personal computer or on hard copy since the transfer occurs over the Internet and it is voluntarily placed into the hands of a third party for storage purposes. This creates a great deal of concern due to the fact that so much personal data is stored online that if stored physically, would be protected (i.e. writing, photographs). While the Fourth Amendment has consistently held that
police must have a search warrant with probable cause to obtain evidence that doesn’t meet any search warrant requirement exceptions. The few cases that have addressed this issue hold that remotely stored digital data has less protections than digital data stored on a home computer or on hard copies (For example Ontario v. Quon, 2010 [search of two employee’s text messages did not violate the Fourth Amendment]; U.S. v D’Andrea, 2011 [web postings are not considered private under the Fourth Amendment]). Current statutes such as the Electronic Communication Privacy Act of 1986 may be too outdated to adequately protect digital papers and effects (active or deleted) and up to this writing, the question of whether deleted cloud data enjoys Constitutional protections has gone unanswered by the courts (Couillard, 2010; Crowther 2012).

While there has been a great deal of research on cloud computing and a person’s expectation of privacy under the Fourth Amendment, there is little extant research on what expectation of privacy an individual has in relation to data deleted from a cloud-based data storage provider. The purpose of this research was to evaluate the impact of the abandoned property doctrine of the Fourth Amendment on personal information and files deleted from the cloud. More specifically, when a user intentionally deletes data stored in the cloud, but a backup copy remains as a normal process of the cloud service maintenance, how does the Fourth Amendment protect the backup copy? How does a user’s expectation of privacy under the Fourth Amendment differ based on specifically where they stored the data they deleted? How does the abandoned property doctrine apply to data deleted from the cloud?

The protection of deleted data should be analyzed via the abandoned property doctrine of the Fourth Amendment. This doctrine holds that an individual must both mentally (intentionally) and physically abandon property for it not to be protected by the Fourth Amendment (Greenwood v California, 1988). When evaluating the abandoned property doctrine to deleted
cloud data, does a person mentally and physically abandon their personal data once they actively delete it from a cloud-based storage provider?

**Literature Review**

**The Fourth Amendment and the Expectation of Privacy**

**Introduction to the Fourth Amendment.** When the Fourth Amendment and Bill of Rights were ratified in 1791, the framers could not have envisioned the technological advancements that have occurred since that time. From automobiles and airplanes to computers and televisions, the technology and even its precursors were outside of mechanic and scientific possibility. However, the framers were smart enough to leave the Fourth Amendment and Bill of Rights vague to account for unknown future advances that may occur. The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” (U.S. Const. amend. IV) The Fourth Amendment is relevant here since its provisions and precedent are what regulates how and what government officials can search.

Unless police officers can articulate that an exception occurred to the warrant requirement of the Fourth Amendment (i.e. exigent circumstances, plain view, consent, search incidental to lawful arrest, vehicle), any searches must be based on warrant with probable cause (Samaha, 2011). Throughout history, this tenet has been the benchmark for Fourth Amendment challenges. The more prominent issue revolves around defining exactly what constitutes a search and it is this question that the courts assess before determining the propriety of the police officer or government official’s actions (Katz v. United States, 1967). For example, an officer might
execute a traffic stop and observe a weapon or drugs on the passenger seat. While the officer is technically (physically) searching when confiscating that evidence, the courts do not consider this a Fourth Amendment search and hence any evidence found would be deemed admissible (Horton v. California, 1990). In other words, the citizen had no expectation of privacy because they left the weapon or drugs in plain view. If that officer searched the trunk of the car without probable cause, it would be considered a Fourth Amendment search since the evidence was not in plain view and the propriety of the search could then be assessed by the courts.

**Evolution of the expectation of privacy.** Prior to 1967, the trespass doctrine was ruling and the courts assessed the reasonableness of searches by stating that only those items that were ‘constitutionally protected areas’ fell under the Fourth Amendment protections. These were the items listed explicitly in the amendment (persons, houses, papers, effects). In other words, police couldn’t trespass into one of these areas without a valid search warrant (Samaha, 2011). If the invasion was outside of these four items, then it would not be considered a Fourth Amendment search and would not be protected. This was a strict interpretation of the Fourth Amendment and an area where the U.S. Supreme court eventually decided more protections for citizens were needed than the trespass doctrine offered (Samaha, 2011).

In 1967, Katz v United States (1967) formed the reasonable expectation of privacy test which fully replaced the trespass doctrine. In Katz, the court determined that telephone eavesdropping was considered a protected search, even when the listening device in question was outside the phone booth Katz used for gambling communications. This test states that a search protected by the Fourth Amendment must have occurred where the citizen had a subjective expectation of privacy and where that expectation is prepared to be recognized as reasonable by society (Katz v. United States, 1967). In other words, it is not enough that a specific person feels
or believes that their actions are private and should be free from governmental invasion. Katz decided that society must also deem those actions to be private. Going back to the traffic stop with a weapon on the seat from the previous example, even if a person believed that the weapon was private, society would not agree because the person left it where a police officer could readily observe it.

If that citizen left that weapon in the trunk, however, the officer could not readily see it. In that situation, society may then agree that the place the officer looked was private and hence protected by the Fourth Amendment. In other words, the court decided that what an individual “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” (Katz, 1967: 351) In making this change, the court went from protecting people not places to protecting people in places, thereby increasing the reach and protections of the Fourth Amendment.

As previously noted, the Fourth Amendment was written in a vague enough manner to allow it to evolve with new technologies that could not have been envisioned by the founders of the Constitution. The expectation of privacy doctrine initially showed promise in this regard. In Smith v. Maryland (1979), the court found telephone users have an expectation of privacy with phone conversations but not with the phone numbers they dial. More recently, the court determined that the use of a thermal imaging device to examine the heat emanating from a building was protected (Kyllo v. United States, 2001). Even though the police did not physically search the house, the use of the thermal imaging device revealed intimate details of actions inside the house and because of this, the court found that Kyllo’s expectation of privacy was reasonable. In another recent case, the U.S. Supreme Court unanimously held that placing a GPS
on a suspect’s vehicle to monitor that vehicle’s whereabouts is considered a search under the Fourth Amendment (Jones v. United States, 2012).

The common thread between these cases is that non-tangible items (phone conversations, heat from buildings, GPS tracking) are considered protected under the Fourth Amendment. This necessarily brings up the question of where the limits of governmental invasion are in relation to online or digital communications. The reasonable expectation of privacy test may be well suited for non-digital items but may be unable to ensure that a citizen’s digital privacy interests are protected from warrantless invasions by governmental officials.

**The third party doctrine and the expectation of privacy.** As elaborated in Katz, this doctrine holds that “what a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.” (Katz v. U.S., 1967: 350), regardless of whether a communication or conversation took place in a private area. Put another way, once a person gives an item to a third person, this doctrine holds that they are voluntarily surrendering their Fourth Amendment protections. The justification behind this doctrine stems from the fact that when a person communicates information to another person, he assumes the risk that the other party will reveal that information to authorities (DeVore, 2010).

In United States v. Miller (1976), the Supreme Court decided that a customer lost his expectation of privacy with his bank records arising from the normal course of business and in Smith v. Maryland (1979), the court similarly held that dialed phone numbers obtained by police from the telephone company were admissible. In both of these cases, the suspect voluntarily shared information with a service provider in order to permit that provider to make a specific service available. The holdings in these two cases “center on the fact that information at issue
was divulged as part of regularly transacted business between the user and the third party, and was kept as a record of such transaction.” (Crowther, 2012: 348)

One of the primary concerns for the applicability of the reasonable expectation of privacy test to the digital realm revolves squarely around the third party doctrine since whenever a person is connected to the Internet, they are knowingly and voluntarily transmitting their data through a third party (their internet service provider). If the data they transmit is meant for the cloud, they are not only transmitting it through a third party but also transmitting it to a third party for storage. Crowther (2012) went further and asserted that there is a gap between what level of privacy individuals expect in digital information and what society is willing to recognize as reasonable. That gap increases as technology advances. The terms of service agreements that people are required to accept undermine expectation of privacy and that judges may lack the technological expertise to adequately apply the doctrine to digital information (Crowther, 2012). Lastly, the U.S. Supreme Court has not yet addressed how the doctrine should apply to data stored by third party providers (2012).
The abandonment doctrine and the expectation of privacy. The U.S. Supreme Court formulated the abandonment doctrine in Abel v. United States (1960), seven years before the Katz reasonable expectation of privacy test was formed. In that case, Abel vacated a hotel room, paid his bill, and turned in his key. Even though he was escorted out by FBI agents, the agents did not have a warrant to search his room. After obtaining permission from the management, they searched the room and found evidence of a crime. The court held that because Abel had fully vacated the hotel room, anything that was left behind was considered abandoned and not protected under the Fourth Amendment (Abel v. United States, 1960).

After Katz was decided in 1976, the abandonment doctrine fell under its auspices and the reasonable expectation of privacy test guided its application. Voluntary conveyance plays a strong role when applying the Fourth Amendment to garbage. The current iteration of the abandonment doctrine asserts that for property to be considered abandoned, there must be an intent to abandon coupled with a physical act supporting the intent (California v. Greenwood, 1988). One must intend to throw away or leave behind property followed by a physical act of throwing away the property or leaving it behind. If this occurs, that citizen’s subjective expectation of privacy would not be considered reasonable by society and that item or property would not be protected under the Fourth Amendment.

The U.S. Supreme Court case of Greenwood v. California (1988) is one of the most cited abandoned property case and aptly describes how the reasonable expectation of privacy test applies to abandoned property. In Greenwood, the police (without a warrant) asked the local trash collector to turn over Greenwood’s trash once they picked it up. Using evidence found in the trash, they secured a search warrant and found evidence of drug possession in Greenwood’s home. Greenwood asserted that he had an expectation of privacy with his trash but the court
determined that his expectation was not one that society would agree with. The court reasoned that Greenwood abandoned his property by placing it on the curb for pickup (California v. Greenwood, 1988). They stated that Greenwood placed the refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through it or permitted others, such as the police, to do so. The police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public (Greenwood v. California, 1988: 43).

Put differently, by voluntarily surrendering their garbage to a third party, a person renounces control over the property (Oppenheimer, 2011).

The decision in Greenwood notwithstanding, there is some disagreement in the lower courts and few have upheld Fourth Amendment protections for trash put out on the curb for collection. For example, courts have found the expectation of privacy remains when one simply places trash on the curb for later pickup (U.S. v. Hedrick, 7th Cir., 1991) or where ordinances prohibit trash picking (State v. Hempele, N.J. 1990). However, the decisions of most lower courts have followed the precedent set forth in Greenwood. For example, in U.S. v Scott (1992), the First Circuit court found that even though Scott had shredded documents found in the trash, it still did not give rise to an objective expectation of privacy. Even though Scott had taken explicit steps to keep the contents from being read, the act of placing his trash in the public domain demonstrated the act of abandonment.

The abandonment doctrine of the Fourth Amendment holds that one loses the expectation of privacy when they intend to and physically take steps to abandon an item (California v. Greenwood, 1988). Abandonment, however, does not equate to destruction. The item or property
still exists in some form but is no longer wanted or needed by the owner and is voluntarily turned over to a third party. This distinction is relevant considering that cloud data may still exist after intentional deletion by the owner.

**Digital Technology: Statutory and Constitutional Protections**

Personal online communications such as email, chat messages, and data generated by online transactions have been regulated via statute and are currently being addressed by the courts. In 1986, the Electronic Communications Privacy Act was passed by Congress to address issues related to digital privacy (ECPA, 1986). However, attempting to apply the Act has been problematic given the significant advances in Internet technology that have occurred over the past twenty-five years. Moreover, appellate courts are generally limited to what issues are brought before them and hence cannot initiate change themselves. Past cases have addressed issues related to advancing technology (Weaver, 2011 for a review) and as shown below in the section on existing judicial precedents, more recent cases have addressed electronic communications. These recent cases have sought to determine the expectation of privacy a person has with their online communications and transactions. Are those communications private and if so, what about when they are in transit via an Internet service provider? Brenner (2005: 3) put it eloquently when she asked, “Can the Fourth Amendment's privacy guarantees be adapted to deal with a world in which technology is increasingly pervasive – A world of ubiquitous technology?” This section will consider this question by briefly outlining the Electronic Communications Privacy Act of 1986 and the positions taken by the courts in relation to these issues.
**Electronic Communications Privacy Act of 1986.** A year after Katz v. United States (1967) decided that governmental interception of telephone calls violated the Fourth Amendment, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968. The act broadened the court’s ruling and prohibited the unauthorized, nonconsensual interception of "wire or oral" communication by government agencies as well as private parties (OCCSSA, 1968). In light of the increasing use of wireless telephone technology, Congress passed The Electronic Communications Privacy Act of 1986 (ECPA). Title II of the ECPA, otherwise known as the Stored Communications Act (SCA), broadened the OCCSSA by adding the prohibition of nonconsensual interception of "electronic communications" by government agencies. The SCA focused on privacy of personal data held in off-site databases and how, while in transit, that data is protected from governmental invasion (ECPA, 1986).

The SCA offers privacy protections in two primary areas. The first set of protections focus on electronic communication services (ECS) and were meant to protect the early, more fragmented form of email as a method of communication (ECPA, 1986). To receive protections from the SCA, an Internet service provider must have the ability to offer users the platform to send and receive electronic communications and have the capability to hold that communication in electronic storage (Robison, 2010). If those two conditions are present, the SCA protects that data. If held in electronic storage for 180 days or less, government agents would require a search warrant to access that data. If held for over 180 days, the government can compel disclosure with either search warrant or a subpoena, the latter offering a much lower level of protection since no judicial oversight is required (Kerr, 2004).

The second set of protections focus on third party service providers that offer remote computing services (RCS). The SCA recognized that users or companies would find it more cost
effective or otherwise desirable to outsource storage of their data to a third party (Kerr 2004). To be eligible for SCA protections, the provider must offer storage capabilities, receive the data electronically, the provider must be used solely for storage purposes, and the provider can only gain access to the data for storage or processing purposes (Robison 2010). If all these conditions are met, the stored data is protected but government officials can gain access with only a subpoena (ECPA, 1986; Couillard, 2009).

The act initially sought to limit governmental wiretaps but was forward looking given that email and remote computer storage was a fairly new technology in 1986. Unfortunately, there is broad consensus that technology has advanced well beyond what the original ECPA envisioned (Burr, 2010). In 2011, the original sponsor of the ECPA (Sen. Patrick Leahy) brought forth a bill to update the SCA by, among other things, limiting access to government officials who possess a warrant based on probable cause. This would have increased the privacy protections currently in place but the bill never made it out of committee (S. 1011--112th Congress: ECPA Amendments Act of 2011). The next section will briefly outline the case law relevant to the continually emerging nature of electronic communications.

**Existing judicial precedents.** When the legitimacy or application of statutes are challenged, resolution falls into the hands of the appellate courts (Samaha, 2011). This is especially important when the issues raised are ones that may not have existed when the statute was initially formed. Over the past decade, the courts have been asked to address issues related to technology and expectation of privacy. While cases related to technology have risen to the appellate courts (i.e. Jones v. United States, Kyllo v. United States), two cases are directly related to government invasions into an individual’s Internet information.
In Warshak v. U.S. (631 F.3d 266, 2010), the Sixth Circuit Court of Appeals ruled that users who store their email with a cloud service provider (i.e. Google) are protected governmental intrusion. Officers must have permission from the subscriber or a warrant based on probable cause. In Warshak (2010), the court also deemed unconstitutional the provision of the Electronic Communications Privacy Act that allows government investigators to use a subpoena or court order issued on less than probable cause to obtain access to emails stored in the cloud. Gubins (2008) even went so far as to call Warshak the Katz of electronic communication. More recently, the Justice Department and Obama administration have asked Congress not to adopt legislation that would place even greater restrictions on governmental access to emails stored in the cloud (Kravetts, 2011) but no new legislation is currently in place.

Web postings are also not considered private under the Fourth Amendment. Katz holds that anything that a person knowingly exposes to the public has no expectation of privacy simply because any other person can gain access and see what was posted (Brenner, 2010). While cases have been decided related to websites that are password protected (U.S. v D’Andrea 671 F.3d 1, 2011) and while many constitutional scholars believe that protections should be present, the courts have not directly addressed whether the Fourth Amendment protects this website information (Brenner 2010). Moreover, the courts have given protection to electronic transactions such as bank transfers or phone call contents since they reveal information that is considered objectively reasonable (Couillard 2009).

1 Conversely, the U.S. Supreme Court ruled that it was not a violation of the Fourth Amendment when a police department punished two officers after an audit of their department issued cell phones revealed inappropriate text messages (Ontario v. Quon 560 U.S. ___, 2010). In this case, the court indicated that the search was reasonably related to work and hence was not a violation of the Fourth Amendment. The concern with this case is that the justices avoided the wider-reaching Fourth Amendment issues and decided this case on very narrow grounds of work related communications. Although this case doesn’t directly address cloud data, privacy groups may find this precedent to be problematic when cloud data privacy based challenges are brought before the courts.
The statutes and decisions previously discussed in this section focus the government’s restrictions when attempting to access a person’s digital communication. The Electronic Communications Privacy Act of 1986 and only a small handful of court cases have addressed issues related to digital privacy. The ECPA of 1986 and the cases never directly address governmental intrusion into a user’s stored cloud data. Moreover, none address the question of how the Fourth Amendment protects data that is voluntarily stored in or deleted from the cloud. A brief introduction to cloud computing must precede this discussion.

Cloud Computing

The National Institute of Standards and Technology defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell and Grance, 2011). Cloud computing allows users to store data on remote servers via the Internet with virtually complete access to that data. A user can gain access to their data even if a copy is not stored on the user’s machine.

In the last five years, cloud computing has become one of the most transformative developments in the history of computers and computing. It has begun to significantly change the way information technology is created, delivered, accessed, and managed (Ruan et al., 2011a). According to Gartner (2009), annual revenue for cloud providers has grown substantially and is expected to reach $150 billion in 2013. On a smaller scale, approximately 69% of online
Americans utilize cloud services\(^2\) (Horrigan, 2008) and of those, there are some users who may engage in criminal activity.

**The cloud and subscriber privacy.** When a user subscribes to and uploads data to a cloud service provider, they must agree to the terms of service of that particular provider. These ‘clickwrap agreements’ require the user to agree to the particular terms of service via a single mouse-click (Calloway, 2011). These agreements set forth the rights between subscribers and cloud service providers. While the subscriber does retain ownership of data that he/she uploads to the cloud, such ownership includes both possession of the data was well as responsibility for information. As Ruan et al. (2012) describes, ownership implies *power* as well as *control* of the data (emphasis added) and who owns the data plays a significant role when law enforcement personnel are attempting to gain access for investigatory purposes. On one hand, the subscriber maintains ownership of the data but the cloud based service provider maintains a level of control (based on the service agreement) that allows for release of that information when legally mandated.

Well known providers such as Dropbox, Google Drive, and Microsoft Skydrive will not release or disclose file or subscriber information when law enforcement simply requests it.\(^3\) Instead, providers indicate that they will release information only when legally obliged to do so. For example, Dropbox will release information and data to “comply with a law, regulation or

---

\(^2\) The Pew Research Center survey defined cloud based services as: Using webmail services, storing personal photos online, using online applications such as Google Documents, storing personal videos online, paying to store computer files online, backing up a hard drive to an online site (Horrigan, 2008)

\(^3\) In February, 2013, the Cyber Intelligence Sharing and Protection Act (CISPA) was re-introduced to Congress. Based on earlier failed versions, this bill would permit private companies and government entities to share information about cyber security threats in the name of national security without legal restrictions. Google, Facebook, and IBM all support CISPA (Spaeth, 2013) but as of this writing, the bill has not been passed and upon passing, it is expected that President Obama would veto the bill (Couts, 2012b).
compulsory legal request.”^4 (Dropbox, 2012: Section 3) Similarly, Google Drive discloses information “necessary to meet any applicable law, regulation, legal process or enforceable governmental request” (Google, 2012: Information We Share). As a third example, Microsoft discloses “to comply with applicable law or to respond to legal process from competent authorities.” (Microsoft, 2012: Section 5.2) Like these three providers, many smaller providers such as Cloudways and Cloud2sMe only disclose information when required by law to do so (Cloudways 2013; Cloud2sMe, 2013). Amazon Web Services, the world’s largest cloud provider, will disclose personal information when “required to comply with the law or requests of governmental entities.” (Amazon Web Services, 2012) This declaration is vague and it is possible that Amazon Web Services could release personal information without being presented with a legal mandate to do so.

Cloud service providers are also seeing an increase in requests from law enforcement for their subscriber’s data. For example, in the last six months of 2012, Google received 8,438 requests from law enforcement agencies in the forms of subpoenas (68%), search warrants (22%) and other court orders (10%) (Bower, 2013). The total number of law enforcement requests of Google in 2012 was 20,938 (Scott, 2012). The increasing number of requests has also led other cloud providers companies, such as Dropbox, to begin reporting law enforcement request statistics in what’s now being called ‘transparency reports’ (Scott, 2012).

**Data deleted from the cloud.** The increasing use of cloud storage requires that users store their online data using a third party. Like physical objects that are thrown away, cloud data

^4 While no specifics are included on the Dropbox terms of service website, it has been reported that Dropbox updated their terms and now require a search warrant when responding to government requests for content information under the Electronic Communications Privacy Act instead of a subpoena (Couts, 2012a).
that a user chooses to delete may not be permanently deleted. In many cases, that data can still be accessed. The data they store may be backed up or duplicated and stored at a mirror site (Oppenheimer, 2011). While this makes sense given the need to protect the data from a disaster or accidental loss, it may also prevent the data from being permanently deleted by the owner.

For example, Dropbox gives directions to allow users to recover data that has been deleted in the past thirty days. If a user upgrades to the paid version of Dropbox and installs the Packrat add-on, they can have access to any deleted files (and any earlier version of each file) for as long as they have the add-on (Dropbox, n.d.). In either case, Dropbox advises that any deleted data will be retained for an unspecified period of time (Dropbox, 2012). Google Drive and Microsoft SkyDrive both require a two-step deletion action by the user, requiring the user to empty their trash after deleting to ensure permanency (Google, 2013; Burt, 2012).

Regardless of how many actions a user must take to ensure permanent deletion, the method by which cloud providers store the data may still allow for recovery. For example, cloud providers (i.e. Google, Facebook) may be more likely to make a user’s data inaccessible rather than deleting it permanently (Schneier, 2009). Additionally, many cloud storage providers are now using snapshots. A snapshot is a process that captures pointers to data blocks and uses them to recreate a data set that may be needed in the future (Slack, 2011). While this serves to be an efficient manner to move data, past iterations of the data are left in the cloud after deletion (Slack 2011).

If data that a user chooses to delete would be immediately and permanently deleted, then there would be no concern about later access from government officials. Unfortunately, this is not the case and data may still be accessible for extended period of time, depending on the cloud provider and the service a user subscribes to. The only way deleted data can be permanently
inaccessible after deletion is if the data was encrypted prior to being uploaded to the cloud. Once the encryption key has been deleted, the data can never be accessed at a later date (Slack, 2011).

**Summary**

The Electronic Communications Privacy Act of 1986 addresses the privacy of digital data but this law was enacted at the beginning of the digital age and its provisions may not be appropriately applicable to the advances technology has undergone since that time (Burr, 2010). As one of those advances, data stored by a cloud service provider may not be adequately protected and concerns arise when a government agent seeks to gain access to that data (Couillard, 2009). Moreover, of the current statutes and few court cases decided that focus on digital data, none have directly addressed privacy concerns associated with stored cloud data that the government seeks access to. As a result, there is little guidance in relation to what expectation of privacy an individual has in relation to data stored and deleted from a cloud-based data storage provider. The next section will examine the implications of the Fourth Amendment on data stored in the cloud and more specifically, the implications of the abandonment doctrine of the Fourth Amendment on data that a user deletes from their cloud service provider account.

**Discussion of the Findings**

**Fourth Amendment Protections for Data Stored in the Cloud**

When thinking about the language of service agreements, it is reasonable to assume that subscribers have voluntarily given up their rights when storing data in the cloud, regardless of whether they fully read the terms of service they agreed to abide by. Based on the current state of jurisprudence, this is only partially correct. The following section will examine how the Fourth Amendment can be interpreted to apply to cloud data.
Generally, police must have a search warrant or probable cause to open closed containers. Since that person has made efforts to keep that information private, they maintain an expectation of privacy that society would deem as reasonable (Samaha, 2011). That subjective and objective expectation of privacy for closed containers is well entrenched in Fourth Amendment jurisprudence since closed containers place a barrier between the potential evidence and the police. However, it must be noted that the court is allowing more container searches based only on probable cause rather than a signed search warrant (Lee, 2010).

The relevance of container searches to cloud data stems from the fact that data stored in the cloud can be seen as a virtual container (Couillard, 2009). The contents are private and a lock, in the form of password protection, encryption, or unlisted link, exists to shield it from the prying eyes of government officials and other citizens. While the digital files are not tangible items, the data those files hold is tangible and it is reasonable to assert that the owner has a subjective expectation of privacy under Katz. In fact, the Court in Katz recognized that intangibles are covered and later lower court decisions have similarly found that digital files are similarly covered (Couillard, 2009). For example, electronic transactions such as phone calls and bank transactions are protected and courts have implicitly recognized that virtual containers do exist (outside of the cloud context) and that they too are protected (Couillard, 2009).

Unlike files stored on a computer, the problem stems from the fact that while the cloud data is in a ‘virtual container’ with barriers preventing public access, the owner has voluntarily given that data to a third party. With the third party doctrine, courts have firmly held that what one exposes to the public is not protected and if the courts were to follow this line of reasoning, it is unlikely cloud data would be fully protected under the Fourth Amendment. Brenner (2009) and Couillard (2009) both agree that the courts will not use this rationale in future cloud data
cases mainly due to the fact that Katz (1967) does allow Fourth Amendment protections for intangible items. Others have not made this direct assertion, believing that privacy protections for cloud users will ultimately be determined by the specific terms of service from the cloud service provider rather than by the level of constitutional protections (Robison, 2010; Calloway 2011). Even when past decisions have held that digital data (held locally) enjoys similar protections as tangible items, there is no general agreement as to rationale(s) appellate courts would adopt when cloud computing cases arise on their docket.

At this point in time, the level of Fourth Amendment protection afforded to cloud data is unclear but in most jurisdictions, cloud data enjoys a lesser level of protection than locally stored data and is governed by the ECPA of 1986 (Couillard, 2010; Harris, 2011). This implies that cloud data enjoys a lesser expectation of privacy. All that is needed for police to gain access to a subscriber’s cloud data is a subpoena\(^5\) (Robison, 2010). While this does constitute a layer of protection from improper police behavior, it is a layer that does not require the approval of a judge (only the prosecutor’s office) (Robison, 2010). In fact, the higher level appellate courts have yet to decide on a case specifically addressing data stored in the cloud (outside of email stored in a cloud-based server).

Based on the literature presented above and court precedent, it is likely that future cases would be decided in favor of the data owner. It is likely the court would assert that the owner of data stored in the cloud does have a subjective expectation of privacy. As noted above, the data is theirs and steps have been taken to shield it from public view. Even though the data is

\(^5\) States and smaller jurisdictions do have the ability to raise the objective basis to require probable cause and a search warrant. Cloud storage providers can require a search warrant but for this type of governmental intrusion, the Constitutional minimum standard requires only a subpoena.
intangible, it is data nonetheless. The deciding factor would likely be the court determining that the expectation of privacy is one that society would recognize as reasonable.

It is plausible to believe the court would find that society would recognize the expectation of privacy as reasonable for several reasons. First, the Fourth Amendment protects persons, houses, papers, and effects against unreasonable searches and seizures. While intangible, it would be difficult to argue that data stored in the cloud was not a personal effect. Second, society would likely agree that when a person password protects information (held locally or in the cloud), they have taken steps to shield that data from public view. Third, it is unlikely that the court would extend the third party doctrine. Even though the owner of the data takes a risk by communicating information to another, they do so with the express and sole purpose of storing data that they maintain ownership over. Lastly, cloud storage providers already restrict access to a user’s data by requiring that they be compelled to release the data (usually via subpoena) but there is a growing trend among providers to require law enforcement officials to obtain a search warrant prior to gaining access (Couts, 2012), a stronger layer of protection.

As the above analysis demonstrates, data that a person stores in the cloud has a layer of protection from police officers (subpoena without judicial intervention) but that protection falls well short of Fourth Amendment standards. Even though there are moves by providers to increase the level of protection, the user’s data is private only so far as the privacy policy provides for. Until the ECPA is updated or until the higher level appellate courts begin to hear cases revolving around the expectation of privacy of cloud data, little is likely to change.

**Fourth Amendment Protections for Data Deleted from the Cloud**

The abandoned property doctrine states that if a person mentally and physically abandons property, they no longer have an objective expectation of privacy that society would deem
reasonable, regardless of whether they believed they had a subjective expectation of privacy. Most cases that are heard in appellate court are for trash that officers have confiscated. While California v. Greenwood (1988) held that trash outside the curtilage does not enjoy Fourth Amendment protections, applying this concept to deleted cloud data raises the question of what is inside (or outside) the virtual curtilage. Couillard described virtual curtilage as follows:

Modern Internet users enjoy access to digital calendars, photographs, address books, correspondence in the form of email messages, and diaries in the form of personal blogs. Such a list may sound familiar—it includes the same materials deemed “highly personal” by the Supreme Court. (2009: 2219)

Currently, physical objects, as well as digital data stored locally are protected by the Fourth Amendment. With no extenuating circumstances present, law enforcement officers must have a warrant or probable cause to gain access to that data and as such, these items are within the virtual curtilage. Many Internet activities, including cloud storage, do not have the same level of protections. Given this, the first step for appellate courts is to determine that cloud data falls within the virtual curtilage prior to making any determination regarding deleted cloud data.

The determination regarding protections for deleted cloud data must be examined in light of the abandoned property doctrine. If the courts determine that the virtual property was abandoned, that person forfeits their Fourth Amendment rights and the evidence obtained is admissible in court. If the courts determine that the property was not abandoned, the evidence obtained is considered the product of a search protected by the Fourth Amendment. Only then can the determination be made as to the admissibility of the evidence. In other words, before

---

6 Curtilage refers to the area immediately surrounding a house. Courts determine whether an item was inside the curtilage by examining the totality of four factors: distance from the house, use of the property, presence or absence of a fence, and measures taken to prevent public view (Samaha, 2011).
assessing admissibility, the courts must determine if a Fourth Amendment search occurred in the first place.

In this analysis, the first question courts ask is whether or not the person had a subjective expectation of privacy with the property in question. With deleted cloud data, it is reasonable to assert that their data is private for several reasons. First, they are the original and only owner of the data. Second, while the data was revealed to the cloud provider, the content was not and the existence of the data was revealed for only storage purposes. Third, once a person deletes their data in the cloud, it is reasonable to believe that no one would have access to it, including the owner. It is likely the courts would find this subjective expectation to be reasonable.

The second question asks whether that subjective expectation is one that society would deem reasonable and to answer this, the abandoned property doctrine must be applied. The first prong of this doctrine asks whether the owner of the data intended to abandon or throw away the data and it is likely courts would determine that the owner did in fact intend to do so. First, the purpose of deletion is to eliminate or erase the data. This implies that the thought behind hitting the delete button was to permanently erase any data that was present. Second, there is a reasonable assumption that the user did not intend to leave a copy of the deleted data behind. Third, it is also reasonable to assert that the intent to delete would not include the thought that the cloud storage provider would keep a copy of that data. These rationales support the assertion that when a user makes the choice to delete data in the cloud, they are of the belief that the data

7 This does not make the assumption that all forms of disposal are equal. As Greenwood made clear, items thrown out and placed on the curb for pickup are then available to the public (i.e. scavengers, animals, small children). Digital data that is deleted on computers is temporarily moved to the trash folder where a second and final deletion of files must be undertaken. When cloud data is deleted, there is an implicit and reasonable assumption that those files would be immediately and permanently deleted.
will be permanently deleted and no further access could be gained by any party. This clearly shows evidence of the intent to abandon.

For property to be considered abandoned under this doctrine the user also must physically take steps to abandon the property in question. On one side, the owner took explicit steps to physically delete the data. They clicked the delete button (and possibly opened the cloud provider’s recycle bin/trash and deleted the data there as well). These are physical steps taken to support the intent to abandon and with that, society might agree that a user has chosen to abandon that property, much like trash. Moreover, a user is expected to have read the terms of service and should be aware what happens to their data once they delete it. If the appellate courts chose to treat deleted cloud data like they do physical trash, it is likely they would deem the data abandoned and acquisition by any government official would be deemed proper.

There is an alternative to this view that courts could subscribe to. This viewpoint may lead the courts to not equate deleted cloud data with abandoned property and hold it protected by the Fourth Amendment. This would stem from two possible viewpoints, the former more plausible an outcome than the latter.

The abandonment doctrine asserts that items one throws away have been abandoned. With physical trash this makes sense, but deleted cloud data can be viewed differently. When one throws out trash, the primary goal is to transfer those items to a third party for disposal. Greenwood stated that while this would generally be the trash collector, scavengers may also take the property for re-use (Greenwood v. California, 1988). The difference lies in the distinction between disposal and destruction.

---

8 If the user deleted data from their local machine, the courts might choose to state that there was no intent to abandon the data since deleting on a local machine is a two step process where data in the trash folder (Mac) or recycle bin (Windows) must also be actively deleted to gain permanency in that deletion.
The goal of deletion is permanent destruction, not disposal or transfer to a third party for disposal. Oppenheimer (2011) asserted that it would be difficult to believe that a user’s choice to delete would imply that the information was meant to be released to a third party for possible reuse. When one returns to the intent of deletion and the goal of permanent inaccessibility, this applies especially to the owner. Unless the owner accidentally deletes the data, it is reasonable to assume that their goal was permanent deletion. Moreover, unlike physical trash, there is an expectation that no one will have access to the data once deleted.\(^9\)

When looking at deleted cloud data from this perspective, one could make the argument that the data itself was not abandoned at all. Instead, there was both the intent and physical actions of destroying the data permanently so no single person could gain access, even the owner. By taking this view, society may be willing to recognize the intent or desire, via destruction, to keep the information private. If they do, then the data would not be considered abandoned and would continue to enjoy the full protections of the Fourth Amendment.

The second but less plausible viewpoint would be for courts to extend the virtual curtilage to include data held offsite but accessible via the Internet from the home. For this to gain legitimacy, courts would be forced to conclude that the Internet was part of the area immediately surrounding the house and hence part of the curtilage (Oppenheimer, 2011). Unfortunately, it is unlikely the appellate courts would extend the virtual curtilage to deleted cloud data when they have yet to extend it to non-deleted cloud data (Couillard, 2010).

\(^9\) However, courts have found that the act of shredding paper prior to throwing it away in the trash did not raise the expectation of privacy. The shredded trash was still considered abandoned and hence law enforcement officials needed no legal justification for obtaining the property (U.S. v. Scott, 1\(^{st}\) Cir. 1992).
Recommendations

Legislation: Updating of the Electronic Communications Privacy Act of 1986

**Cloud data as RCS.** Distinctions should be made placing cloud data in the RCS or remote computing services category. ECS, or electronic computing services, was meant to cover the early forms of email and while the provider must have the ability to store the data electronically, that storage is incidental to electronic transmission (Robison, 2010). RCS focuses more on remote storage of the data. So rather than holding the data that will be transmitted, RCS requires that the data be stored or maintained for the owner by a provider whose sole function is to provide electronic storage (Robison, 2010). While under the ECPA of 1986, this currently allows for fewer protections than if cloud data was considered ECS, it is clearly the proper designation. Once that proper designation is made, individual judges will not be forced to decide the data’s status and hence the proper level of protection. Couillard (2009) believes that cloud data will likely be considered RCS under the ECPA of 1986, but that consistent designation will only be the first step toward appropriate revision and modification of the ECPA. This change would bring clarity to a law that is in need of updating.

**Search warrants to gain access to cloud data.** Currently, the ECPA requires law enforcement officials to obtain a search warrant only when they seek to gain access to ECS that has been maintained for 180 days or less. For ECS maintained over 180 days or for RCS data, government officials may choose to obtain a search warrant but a court order or subpoena is all that is necessary to compel disclosure (ECPA, 1986). Any update to the ECPA should include a minimum search warrant requirement for both categories without regard to time limitations. The exponential increase in both private and corporate use of cloud data storage could not have been envisioned when this law was enacted. More and more, people are willing to upload their data to cloud storage providers but for the sole purpose of storage, not sharing. It is reasonable to expect
that the owners of the stored data would believe that their information is private. Under Katz, that expectation should be recognized as reasonable by society, thereby affording it the full protections of the Fourth Amendment. Couillard (2009) agreed, asserting that data in the cloud should be considered within the virtual curtilage and as such, it should enjoy the same protections that its tangible counterparts currently enjoy.

**ECPA protections for deleted cloud data.** The previous recommendations focus on non-deleted cloud data and as noted, limited protections are in place under the ECPA. The ECPA, however, does not protect data that has been deleted nor is there any appellate court decision that focus on protections afforded to deleted cloud data. Any revisions to the ECPA of 1986 should include provisions that protect deleted cloud data. While an argument can be made that it has been abandoned by its owner, the very act of deletion signifies that the owner sought to permanently destroy the data, making it inaccessible to anyone. The act of deletion differs from throwing trash away since the trash can be accessed later as explicitly noted in Greenwood (1988). Permanent deletion indicates that the owner wanted that data to be kept private from any prying eyes. Appellate courts will likely hear cases in the future but a revision of the ECPA should include provisions to protect deleted cloud data and recognize it as private.

**Cloud Storage Provider Duty: Deletion Should Equal Deletion**

When a user deletes data, they expect that data to be permanently inaccessible, even if they must go through a two step process of deleting the data, and then emptying of the recycle bin or trash. When an owner deletes data stored in the cloud, that data may not be irretrievable. Snapshots may be kept: the data may not be immediately deleted, and may only be overwritten at a later time by the provider when space is needed. This facet of cloud storage is where the crux of the issue lies. If providers permanently deleted the data immediately upon the owner’s
command, no further protections against governmental intrusion would be needed because the data would no longer exist.

**Fourth Amendment Protections for Deleted Cloud Data**

As this analysis shows, courts should afford Fourth Amendment protections to deleted cloud data. If the current environment in Congress remains, there is less likelihood that the ECPA of 1986 will be updated. If that does not occur, the burden will fall onto the appellate courts to interpret the ECPA to determine the level of Fourth Amendment protection. That interpretation should include determinations that cloud data is RCS and that deleted cloud data is still considered owned data until it is permanently destroyed. With these designations, both would be considered protected under the Fourth Amendment.

If courts determine that deleted (but not destroyed) data is still owned data, they would have extended the virtual curtilage to data in the cloud. While reluctant to do so (Oppenheimer, 2011), the Supreme Court has made the distinction between a container and its contents. Exposing the former to the public does not surrender the privacy rights of the latter (Horton v. California, 1990). So while a person may upload data in the cloud and expose the transmission information (i.e. email header, IP addresses) to a third party, the contents of the upload should remain private. Deleted data, if still accessible by the owner or provider, should still be considered as contents of a virtual container.

**Judicial Education and Training**

Like many professions, in-service training programs for judges exist. Unfortunately, most programs focus on general legal issues and education than specific technology related education. This makes sense given the proportionally few cases where emerging technology and the Fourth Amendment are intertwined. The more judges that are trained to understand emerging
technologies, the more prepared they will be when these types of cases arise. There is precedent for this since it is akin to the specialized courts that are present in many individual states and at the federal level. These include juvenile courts, domestic violence courts, and drug courts, among others. Since there is precedence for judges who are specialized in a single topical area, it makes sense to allow technology cases to be heard by a judge who is educated enough in these matters to make informed decisions in that case.

It must be recognized, however, that this could become problematic since appellate court judges hear appeals as a group rather than individually. A single judge in an appellate case would be required to instruct other judges on emerging technology and the law. A problem arises since the way that a specific judge understands the technology and how knowledge is conveyed could have a negative influence on those other judges. For example, an appellate judge could deem cloud data as ECS rather than RCS and that might impact a decision if the law enforcement officers did not obtain a search warrant prior to obtaining cloud data evidence. While limitations are present with this approach, it is one that is worthy of exploration.

Further Research

It seems unlikely that the ECPA of 1986 will be updated anytime soon. Even if it is updated, it is unlikely that it will go so far as to protect deleted cloud data. With that in mind, the courts will likely become the primary arbiter of law. Future research would be smart to examine court decisions on a much more finite level. For example, it would be difficult to imagine that trial courts have not made decisions on motions to suppress cloud data (or deleted cloud data) that was obtained without a search warrant. Moreover, these issues may also have been heard in lower level appellate courts (i.e. state courts) and while these are less likely, an analysis into various state jurisdictions is recommended.
Unfortunately, even with an analysis of lower court appeals and motion hearings, the outcome remains the same. Without the U.S. Supreme Court ruling for or against the protections for deleted cloud data, any analysis relies on conjecture, albeit informed conjecture. The benefit of these types of studies revolves around understanding the larger picture of this data and Constitutional protections. If lower courts are deciding in favor of protection, then the higher level appellate courts may see this as society’s recognition of a person’s subjective expectation of privacy with deleted cloud data, and that may lead to a stronger level of Fourth Amendment protections.

Conclusions

The statutes in place and court decisions make one thing abundantly clear: Digital data stored remotely enjoys a lesser expectation of privacy than digital data stored on a person’s local machine or tangible items held by a person. Whether text, email, or cloud data, law enforcement officials may be able to gain access to these types of data with a subpoena or court order rather than a search warrant based on probable cause. Current statutes such as the Electronic Communications Privacy Act of 1986 may be too outdated to adequately protect digital papers (Crowther, 2012), and the higher level appellate courts have not been faced with a Fourth Amendment cloud data case or one that involves law enforcement access to deleted cloud data.

This research delved further than the statutes or court decisions have. The purpose here was to evaluate the impact of the abandoned property doctrine of the Fourth Amendment on personal data deleted from the cloud. More specifically, when a user intentionally deletes data stored in the cloud, what level of Fourth Amendment protections should exist for that data? In other words, how does a user’s expectation of privacy under the Fourth Amendment differ based on specifically where they stored the data they deleted? The abandoned property doctrine was
used to assess the expectation of privacy an individual has in relation to data deleted from a cloud-based data storage provider.

The analysis presents a clear path toward appropriate Fourth Amendment protection of deleted cloud data. It was shown that by applying the abandoned property doctrine, deleted cloud data could still hold that expectation of privacy and that it would be one recognized as reasonable by society. Unlike trash, the intent to permanently and immediately destroy the data differs from the intent and act of turning over the data to a third party for disposal. This crucial distinction is one that courts can rely on when deciding cases where a petitioner alleges a Fourth Amendment violation via law enforcement access of deleted cloud data.

Many obstacles will be present prior to courts making this determination. Cloud data (undeleted) must be first categorized as RCS. Second, RCS must be afforded a higher level of Constitutional protection from governmental intrusion, accomplished either through legislative act or appellate court decision. Finally, the role of the third party doctrine applied to cloud data must be reconciled and determinations must be made that protect the contents of the virtual container even if the container itself is visible to a third party. The road to Constitutional protections for deleted cloud data is a long one but given the continuing increased utilization of cloud storage, it is a road that must be traveled.
References


Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (2011b, April 6). *Survey on cloud forensics and


U.S. Constitution Amendment IV.


**Statutes Cited**


United States v. D’Andrea 671 F.3d 1, 2011