North Dakota Law Review

Volume 90 | Number 1 Article 6

1-1-2014

The Sky's the Limit: Twenty-First Century Searches of Hard-Drives, Smartphone Applications the Cloud

Quinn Hochhalter

THE SKY'S THE LIMIT: TWENTY-FIRST CENTURY SEARCHES OF HARD-DRIVES, SMARTPHONE APPLICATIONS, & THE CLOUD

ABSTRACT

Now more than ever, computers and smartphones are used to store much of our personal information. It is no coincidence that these devices are being increasingly used in criminal investigations. This Note reviews current trends in the searches of electronically stored information, considers alternative proposals, and reviews current Supreme Court speculation. Specifically, this Note looks at the differences in search protocol depending on where digital information is stored: either on-site, such as a hard-drive or disk, or off-site, such as a smartphone application or in the cloud. Understanding where and how virtual information is stored will help to ensure the legal community makes informed decisions as it continues to develop this area of law.

I. INTRODUCTION

The alarm on your cellphone rings. It's 7:00 a.m. Time to get up and get ready for work. Before you leave the house, you check your personal email. You check your work email. You check your phone's text messages. You record your jog in your smartphone's fitness application.[1] It only takes a second. Your smartphone remembers you. Your smartphone remembers all of your account information, no passwords necessary. On your way to work you access your music downloads and call a nearby dentist to schedule an appointment. When you arrive at work you

1. "A mobile application is a piece of software that is contained within a phone for a particular purpose or use . . . Essentially, the main goal for all mobile applications is to provide a service that can be used on cell phones rather than an actual computer." Alex Krouse, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731, 732 (2012).

take a picture of the early morning sunrise and upload it to Instagram,[2] complete with the time of day and your geographic location.[3] In the elevator, you read reviews of new lunch spots in the neighborhood. Google predicts your search based[4] on your previous searches and you passingly acknowledge that the advertisements in the margins are tailored to items you have recently searched or purchased online.[5] Just as you are about to sit down at your desk and get to work, you fire off a last minute reply message to a Facebook friend.

Our phones and our laptops know more about us than ever before. Each year, technology is greatly improving the ease and speed with which we document and record our daily lives.[6] In fact, because of the ease and convenience with which it can now be done, it may be that people record and keep information that they otherwise would not have kept.[7] The only real limit on the amount of information stored used to be based upon the device's storage capacity, but now with the introduction of remote storage locations, like Apple's iCloud,[8] the virtual sky is the limit. Aware that more and more personal information is stored with their products, many electronic manufacturers offer password protection[9] for their devices, which users may or may not choose to use. Security features such as numerical

---

2. Instagram is a photo-sharing service owned by Facebook.

3. *Privacy Policy*, INSTAGRAM, www.instagram.com/about/legal/privacy/#section1 (last visited Jan. 6, 2014):

> Users can add or may have Metadata added to their User Content . . . This makes . . . User Content more searchable by others and more interactive [and] your latitude and longitude will be stored with the photo and searchable . . .if your photo is made public by you in accordance with your privacy settings.

4. Google completes searches and URLs typed into Google Chrome's address bar similar to autofill in web forms. *Google Chrome Privacy Notice*, GOOGLE, https://www.google.com/intl/enUS/chrome/browser/privacy/ (last visited February 21, 2014).

5. Google collects information from its user's browsing activity and uses the information to provide custom advertisements. *Ad Targeting: About Internet Based Advertising*, GOOGLE, https://support.google.com/adsense/answer/113771?hl=en (last visited February 21, 2014).

6. Fifty-seven percent of American Adults use their cell phone to go online. Twenty-one percent of cell phone owners say they mostly access the internet using their phone. Maeve Duggan & Aaron Smith, *Cell Internet Use 2013,* PEW RESEARCH (Sept. 16, 2013), www.pewinternet.org/topics/Mobile.aspx?typeFiler=5.

7. Google's Gmail users with empty trash folders used to receive messages such as: "No conversations in the trash. Who needs to delete when you have 1000 MB of storage?!". *See* Ari Schwartz, Deirdre Mulligan & Indrani Mondal*, Storing Our Lives Online: Expanded E-mail Storage Raises Complex Policy Issues*, 1 I/S: J.L. & POL'Y INFO SOC'Y 597, 601 n.7 (2005).

8. "iCloud lets you access your music, photos, documents, and more from whatever device you're on . . . iCloud puts your content on all your devices." *iCloud*, APPLE www.apple.com/icloud (last visited Jan. 6, 2014).

9. Typical passwords for mobile devices are numerical or picture drawing sequences. Recently, Apple released a new iPhone which is fingerprint protected. On the iPhone 5s, the Touch ID sensor quickly reads your fingerprint and unlocks your phone. *Iphone 5s*, APPLE, www.apple.com/iphone-5s/features/ (last visited Feb. 15, 2014).

passwords have long been used to hide your device's contents from prying eyes in the event that it becomes lost or is stolen. As long as your smartphone is password protected, you do not have to fear that someone will find out just how many photographs of those venti, soy lattes you have been taking.

Most smartphones, though, contain more than just pictures of artistically designed latte foam. As alluded to earlier, a smartphone is often used for a lot more than just its camera. Any one smartphone or laptop device may contain hundreds of pictures, emails, documents, and other digital information on its own hard drive. Many devices also have access to many more files that can be located or saved remotely. The amount of information that is accessed through each of these devices makes recording and documenting our lives easier and, not coincidentally, makes fighting crime easier as well. With regards to criminal activity, a computer can be used to store illegal contraband, such as child pornography, evidence of criminal activity, such as a record of illegal transactions or fraud, or as the instrument of a crime.

Although it is now common for investigators to search and seize electronic devices, questions about what is reasonable or what is fair still remain. Rapid advances in the way technology can record, save, and duplicate mass quantities of information may prove difficult to deal with for a profession that prefers to act only where there is precedent. Until the Supreme Court addresses this issue directly, the current trend has been to apply established search and seizure law to searches of electronic devices. Using doctrines intended for limited physical spaces, possessions, and time frames, however, is cause for concern where they are applied to such huge quantities of information contained in virtually limitless boundaries.

In order to aid North Dakota's legal community in making informed decisions while developing this area of law, this Note provides an overview of how electronic information is being stored, how the law is currently being applied to these technologies at both the state and federal levels, and alternative proposals that have been made in anticipation of future Supreme Court review. It is my hope that a better understanding of how electronic information is being stored, combined with the lawyer's understanding of how this information is typically used by lay citizens and criminal investigators, will lead to tailored, fair, and just laws consistent with the reasonableness requirement of the Fourth Amendment.[10]

10. The Fourth Amendment of the United States Constitution states that:
[t]he 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

II. ELECTRONIC STORAGE

The amount of information that can be stored electronically is really astonishing. If you are shopping for a new laptop, you will find that most devices offer 100 to 300 gigabytes (GB) of storage space on their hard drives. To give you an idea of how much information that is, a LexisNexis chart indicates that a single GB is equivalent to approximately 64,782 pages of Microsoft Word files.[11] Any items saved to the laptop will be located in the hard drive; this does not include email. These days, email is typically held in third-party storage. For example, Google offers its Gmail users fifteen GB of free, internet-based storage with each email account.[12] Fifteen GB of storage is fifteen times what Google offered Gmail users ten years ago.[13] Additional storage, should you need it, is easy to come by. External hard drives (often offering one or two terabytes of storage),[14] thumb drives, compact discs (CDs), and third party or web-based, cloud storage are relatively inexpensive ways to dramatically increase electronic storage capacity.

Since electronic storage is often out of sight, it often stays out of mind. Anyone storing hundreds of thousands, or even tens of thousands of documents in their home office would likely draw some criticism from their housemates. That is not the case if the documents are stored electronically. When we are not forced to organize and find spots for physical files, we no longer need to be concerned with exactly where they are located. For example, those of us using Apple's Macbook know that our pictures and videos are saved in iPhoto, our music is saved in iTunes, and our emails are in Messages, but knowing where to click and knowing where a file is saved are not the same. Many people may not realize that while some of their files are being saved locally, directly to their computers or on-site, others are being kept remotely, online on a third-party server or off-site.

A. ON-SITE STORAGE

I will refer to the files saved to a computer or other closed container as on-site, meaning the information's source is kept locally, inside the device.

---

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.

11. *How Many Pages in a Gigabyte?*, LEXIS NEXIS 1, 1 (2014), www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adifspagesinagigabyte.pdf.

12. *Google Drive*, GOOGLE, www.google.com/drive (last visited Jan. 4, 2014).

13. *See* Schwartz et al., *supra* note 7, at 600.

14. A terabyte is a measure of storage capacity equal to 1,000 GB. The prefix "tera" is Greek for "monster." *Tera*, MERRIAM WEBSTER, www mirriam-webster.com/dictionary/tera (last visited Jan. 4. 2014).

For example, files saved to external hard-drives or thumb drives store information locally. Information kept on these storage devices is typically owned or used exclusively by one individual, though that individual is likely to have no idea how the information is being recorded. While they come in many different forms, computers storage devices operate similarly. Specifically, the hard drive stores information in various eight-character strings of zeroes and ones.[15] As one commentator explains:

> The hard drive itself consists of several magnetized metal platters, something like magnetized compact discs that contain millions or even billions of tiny magnetized points placed in concentric circles like the growth rings of a very old tree. The magnetized points can be left either in a magnetized state, which represents "1," or a demagnetized state, which represents "0." Whenever a user enters a command that requires the computer to access data stored on the hard drive or write data onto the hard drive, the platters spin and the magnetic heads are directed over that portion of the hard drive where the particular information is stored. As the magnetic heads pass over the magnetized points on the platters, they generate an electrical current. That current is the signal representing the zeros and ones and can be inputted into the computer processor or outputted from it.[16]

Searching on-site information is perhaps more similar to traditional physical searches of a home than off-site information because the on-site files are actually located within a contained space to be searched. It is clear, however, that even on-site files are much more complicated and vast than anything that could be physically contained in a house. When we try to decide what it means to search and seize this type of information, it may be important to consider just how different the physical and the electronic realms are. Only the device's user, as opposed to the general public, typically accesses on-site files, but it is not necessarily the case that the user has complete control over those files. Just as many users do not fully understand how their computer data is stored, many users do not know when their data is deleted.

> For example, forensic analysts can often recover deleted files from a hard drive. They can do that because marking a file as "deleted" normally does not actually delete the file; operating systems do not "zero out" the zeros and ones associated with that file when it is

15. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538 (2005).

16. *Id.* at 539.

> marked for deletion. Rather, most operating systems merely go to the Master File Table and mark that particular file's clusters available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer is analyzed, the file marked for deletion will remain undisturbed. Even if another file is assigned to that cluster, a tremendous amount of data often can be recovered from the hard drive's "slack space," space within a cluster left temporarily unused. It can be accessed by an analyst just like any other file.[17]

Just because we *can* keep tens of thousands of files does not mean we *want* to. Similar to the way we clean up our homes, many of us organize, sort, and clean out our old documents, music, and emails from time to time. Interestingly, however, the intent we have to get rid of or destroy our electronic data is not necessarily enough to make it so. Our files may remain in our possession without us even being aware of them.[18] Many device users may incorrectly assume that if they can no longer see the file, then nobody else can either. In an age where more and more of our lives are conducted electronically, this type of data recollection may prove invaluable to law enforcement as they conduct criminal investigations. There is arguably no other place a law enforcement officer can search where he has such a great opportunity to look into someone's past the way he can with an individual's computer history. An interesting consideration then becomes whether this type of data recollection serves the interests of justice by preventing an individual from destroying what may potentially have been evidence of a crime, or whether this type of data recollection hinders justice by taking advantage of an individual's unfamiliarity with advancing technology.

B. OFF-SITE STORAGE

Data can also be stored remotely, in the cloud.[19] The cloud is a network of servers or, in other words, the internet. Remote storage is becoming preferable because of its seemingly unlimited capacity and its ability to be accessed from anywhere.[20] Off-site storage is often third-party

17. *Id*. at 542.

18. *Id*.

19. Cloud computer refers to an architecture that links computers in a grid and allows users to access data or processing power. Storing photos on the web or accessing webmail are two examples of cloud computing. Janna Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW RESEARCH (June 11, 2010), www.pewinternet.org/Topics/Technology-and-Media/Cloud-Computer.aspx?typeFilter=5.

20. "[Fifty-one percent] of internet users who have done a cloud computing activity say a major reason they do this is that it is easy and convenient." John Horrigan, *Use of Cloud*

storage. Rather than saving your data to your own device, you are saving the data to a third-party server.[21] Despite its growing prevalence, it seems that the average electronics user understands even less about this type of storage than he or she may understand about on-site storage. In fact, many people do not even realize they are using the cloud. Citrix, reporting on a Wakefield Research poll conducted in August of 2012, announced that:

> A majority of Americans (54 percent) claim to never use cloud computer. However, 95 percent of this group actually does use the cloud. Specifically, 65 percent bank online, 63 percent shop online, 58 percent use social networking sites such as Facebook or Twitter, 45 percent have played online games, 29 percent store photos online, 22 percent store music or videos online, and 19 percent use online file-sharing. All of these services are cloud based. Even when people don't think they're using the cloud, they really are.[22]

Whether we are consciously aware of it or not, cloud-computing seems to be taking over. The annual North Bridge Future of Cloud Computing Survey reported that seventy-five percent of companies used the cloud in 2013.[23] This figure represented an increase from the sixty-seven percent of companies that used the cloud in 2012.[24] The cloud means that we can now store more information than ever before and the polls mean that more people are using the cloud every year, whether they know it or not. Whether or not they are aware of it, people who access smartphone applications and websites such as Netflix, Facebook, Dropbox, or Google Docs are using the cloud. This type of information storage is even less similar to the traditional physical searches than computer hard drives were. It may become necessary for the legal community to reevaluate traditional search and seizure law in light of how our personal information is now commonly used and stored, while keeping in mind what the average user knows or does not know about the devices and data he or she is using.

Computing Applications and Services, PEW RESEARCH (Sept. 12, 2008), www.pewinternet.org/2008/09/12/use-of-cloud-computing-applications-and-services/.

21. The third party server will depend on the website you are using; popular third parties include Google's gmail, Apple's iCloud, or websites, such as Facebook.

22. *Most Americans Confused By Cloud Computing According to National Survey*, CITREX (August 28, 2012), www.citrix.com/news/announcements/aug-2012/most-americans-confused-by-cloud-computing-according-to-national html.

23. *The Future of Cloud Computing 3rd Annual Survey 2013*, NORTH BRIDGE, www nbvp.com/2013-cloud-computing-survey; *see also* Michael J. Kok, *2013 Future of Cloud Computing 3rd Annual Survey Results*, www.mjskok.com/resource/2013-future-cloud-computing-3rd-annual-survey-results.

24. *See generally* Kok, *supra* note 23.

III. ELECTRONIC SEARCHES & THE LAW[25]

The Fourth Amendment of the Constitution protects citizens against unreasonable searches and seizures.[26] It was important to the authors of the Fourth Amendment to include a particularity requirement in the language of the Fourth Amendment, which prevents law enforcement officials from executing general searches. Warrants must describe specifically where, when, and what police officers are searching for and they are approved by a judge prior to execution. This means that if the police are searching specifically for a large object, they may not look for it in small areas that would be unable to contain the larger object, because that would be unreasonable.[27] The touchstone of the Fourth Amendment, in other words, is reasonableness.

As interpreted by the Supreme Court, the Fourth Amendment is a protection of people, not places,[28] and offers protection where an individual has a "reasonable expectation of privacy."[29] The reasonable expectation of privacy test asks whether the individual exhibited a subjective expectation of privacy with regard to the thing searched and, if so, whether that expectation of privacy is one that society is prepared to recognize as reasonable.[30] Since electronic stored information is relatively new, the majority of case law surrounding the Fourth Amendment concerns the searches of homes and physical possessions. The case law in this area makes sense with regards to physical searches because warrants describing a specific address, room, and object to be searched within a given time period offer the detailed particularity necessary for a citizen's protection. As applied to electronically stored possessions, which store vast quantities of information in locations unfamiliar to law enforcement, prosecutors, and magistrates, these specifications may make less sense and may ultimately be less reasonable.

Courts have likened an individual's expectation of privacy in his or her computer to the expectation of privacy held in other closed containers.[31] Similarly, CDs[32] and individual computer folders[33] have been found to

25. Electronic evidence is typically governed by the Fourth Amendment of the U.S. Constitution and statutory laws codified at 18 U.S.C. §§ 2510-22 (2006), 18 U.S.C. §§ 2701-12 (2006), and 18 U.S.C. §§ 3121-27 (2006).

26. U.S. CONST. amend. IV.

27. *Id.*

28. Katz v. United States, 389 U.S. 347, 351 (1967).

29. *Id*. at 360 (Harlan, J., concurring).

30. *Id*. at 361.

31. United States v. Ross, 456 U.S. 798, 822-23 (1982).

32. *See* United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2011) (holding that police may examine remaining files on a disk that had been partially, privately searched).

represent a closed container for purposes of Fourth Amendment analysis. Even so, some courts have explicitly acknowledged the significant differences between electronic storage devices, like computers, and typical closed containers, such as briefcases or folders:

> The advent of the electronic age and . . . development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law.[34]

Remotely stored folders, however, may not be considered closed containers the way on-site folders are. The Supreme Court has held that there is no Fourth Amendment protection where personal information is kept by a third party because there is no reasonable expectation to privacy where information is shared with or given to a third party.[35] What does that mean in the age of cloud computing and smartphone applications? As described earlier, more and more of our internet-based activities require using third party, cloud based storage, whether we are aware of it or not. How will the law resolve whether an individual maintains his or her reasonable expectation of privacy when the contents of his accounts are (and perhaps must be) stored with third party providers?[36] Even if an individual has a reasonable expectation of privacy in the stored information held by a third party, if the third party has common authority over the information, it may choose to disclose it to the government itself.[37]

---

33. *See* People v. Emerson, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) (holding computer folders rather than files are closed containers).

34. United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

35. *See* United States v. Miller, 425 U.S. 435 (1976) (holding that financial records kept by a bank were outside the protection of the Fourth Amendment); Couch v. United States, 409 U.S. 322 (1973) (holding that a subpoena for records provided to an accountant from a client for the purpose of preparing tax returns did not raise a Fourth Amendment issues); United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002) (holding there is no reasonable expectation of privacy in information placed on the internet); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (holding individuals have no expectation of privacy in dialed phone numbers).

36. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-08 (9th Cir. 2008) (holding a reasonable expectation of privacy exists in paper messages stored by provider of communication services); *see also* Wilson v. Moreau, 440 F. Supp. 2d, 108 (D.R.I. 2006) (holding a reasonable expectation of privacy exists in a Yahoo! email account).

37. *See* United States v. Young, 350 F.3d 1302, 1308-09 (11th Cir. 2003).

A. STATUTORY LAW: THE DEPARTMENT OF JUSTICE'S APPROACH TO ELECTRONIC SEARCHES

At the federal level, the applicable law for searching electronically stored information will vary depending on where the information sought is located. For on-site, locally held data, law enforcement will seek a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.[38] For off-site, remotely held data, varying statutory provisions, such as the Electronic Communications Privacy Act[39] (ECPA), may be controlling.

1. On-Site

Similar to the search of a home, Rule 41 of the Federal Rules of Criminal Procedure typically governs searches of on-site electronic data. This practice of treating electronic searches similar to physical searches has caused a debate about how the plain view doctrine[40] is implicated. As we know, computers hold a lot more information than the typical household file cabinet. In fact, computers likely hold more information than the average user even knows about:

> Metadata and other artifacts left by the computer can reveal information about what files have recently been accessed, when a file was created and edited, and sometimes even how it was edited. Virtual memory paging systems can leave traces of information on the hard drive that the user might have believe was stored only in volatile computer memory such as RAM and expected to disappear when the computer was shut down. Browsers, mail readers, chat clients, and other programs leave behind configuration files that might reveal online nicknames and passwords. Operating systems and applications record additional information on the hard drive, such as records of Internet usage, the attachment of peripherals and flash drives, and the times the computer was in use. Collectively, this information can reveal to an investigator not just what a computer happens to contain at the time of the search, but also evidence of who has used a computer, when, and how.[41]

---

38. Fed. R. Crim. P. Rule 41.

39. *See* 18 U.S.C. §§ 2510-2522 (2006).

40. The plain view doctrine is an exception to the Fourth Amendment's warrant requirement. Specifically, it allows law enforcement officers to seize objects with an immediately apparent incriminating nature, so long as the officer is lawfully in the place from which the object was seen. *See* Horton v. California, 496 U.S. 128 (1990).

41. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUSTICE, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 62 (2009) (hereinafter referred to as "DOJ Manual").

The sheer volume of information accessible in on-site searches has caused some in the legal community to wonder if the plain view doctrine, as applied in these circumstances, is effectively swallowing the entire warrant requirement. In a computer search, however, it is unlikely that law enforcement officers or investigators will know exactly where they need to look (especially when criminals hide or encrypt files). So what can law enforcement look at? The Department of Justice (DOJ) takes the position that its investigators may make a cursory review of each file on the computer to first determine whether or not it falls within the scope of the search warrant.[42] Oftentimes, an investigator who inadvertently discovers evidence of a new crime (in plain view) on the device will seek an additional search warrant authorizing a search for the new crime. This may be a safe practice for now, but some courts remain concerned because of the overwhelming amount of information stored on these devices and have instead required officers to use taint teams[43] or waive the plain view doctrine entirely.[44]

It is worth mentioning that in 2012, North Dakota amended its criminal code to provide for warrant guidelines authorizing seizures of electronically stored information and its storage mediums. Specifically, it provides that:

> A warrant under Rule 41(c) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.[45]

This language indicates an approach similar to that of the DOJ in that law enforcement can look first and what they find can be reviewed later. It is likely that this approach implicates similar plain view doctrine concerns as those previously discussed.

---

42. "The plain view doctrine arises frequently in the search warrant context because it is usually necessary to review all files on a computer to find evidence that falls within the scope of a warrant." *Id.* at 36; *see also* United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006) (holding too much evidence could escape discovery if warrants were limited to specific search protocol).

43. "A team of prosecutors . . . may form a 'filter team' or a 'taint team' to help execute the search . . . The filter team sets up a so-called 'ethical wall' between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall." DOJ Manual, *supra* note 41, at 110.

44. "Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases." United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009).

45. N.D.R.Crim.P. 41(c)(2)(3).

2. Off-Site

The Stored Communications Act ("SCA")[46] regulates the government's access to stored account information from network service providers by providing statutory privacy rights for users of computer network service providers. The SCA provides protection in relation to the importance of the privacy interest at stake: "some information can be obtained from providers with subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not."[47]

The rules of the SCA must be applied to the facts of each case. Agents and prosecutors must classify the network provider by its service, classify the information sought as enumerated by the SCA, and consider whether they are seeking compelled or voluntary disclosure by the provider.[48] If a prosecutor decides to seek compelled disclosure, she must determine whether a search warrant,[49] a 2703(d) court order,[50] or a subpoena is necessary to do so. The differences between these methods of disclosure lies in what the government must show in order to gain access to the sought after information. For example, if the DOJ wants to obtain something such as call logs, it only needs a 2703(d) court order, which only requires that the government show that there are reasonable grounds to believe that such information is relevant to an ongoing investigation. This, in other words, is less than a showing of probable cause. If, on the other hand, the DOJ is seeking the content of those calls, it usually needs to obtain a search warrant, which requires a showing of probable cause.

B. CASE LAW: ELECTRONIC SEARCHES IN THE DISTRICT OF NORTH DAKOTA

Compared to that of traditional, physical searches, there is relatively limited case law for electronic searches. There is even less developed case law in North Dakota. This absence should be recognized as an opportunity for our state to start on the right foot. As our economy continues to grow and as remotely located electronic storage becomes increasingly prevalent,

46. The SCA is included in Title II of the Electronic Communications Privacy Act of 1986 ("ECPA") and are often referred to interchangeably. 18 U.S.C. §§ 2701-2712 (2006).

47. DOJ Manual, *supra* note 41, at 116.

48. *Id.*

49. This search warrant would still have to comport with N.D.R.Crim.P. 41.

50. "[A] 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some)." DOJ Manual, *supra* note 41, at 127.

our courts will likely be presented with new legal questions about what it means to protect a North Dakotan's right to be free from an unreasonable search. As always, we will look to precedent when we are confronted with new challenges. For this purpose, this article addresses two cases from the federal courts of North Dakota that offer insight on what a reasonable electronic search looks like at the federal level.

1. United States v. Mutschelknaus

In *United States v. Mutschelknaus*,[51] Chad Allen Mutschelknaus moved to suppress evidence found on his computer and electronic storage media after he was indicted for receipt and distribution of material involving the sexual exploitation of a minor.[52] From a computer in Mandan, North Dakota, Mutschelknaus sent over 200 pictures during an online conversation with an undercover agent.[53] Two months later, the special agent submitted a warrant application to search the Mandan residence and "any computer/electronic storage media that may be seized."[54] The resulting warrant provided that the search be conducted by December 22, 2007 and granted the government the right to search any authorized electronic device or storage media sixty days from the warrant's execution.[55] The agents performed the forensic analysis of Mutschelknaus' computer and storage media between December 14, 2007 and February 12, 2008.[56]

Mutschelknaus moved to suppress the warrant, arguing that the special agent did not establish probable cause in the warrant application. Specifically, Mutschelknaus pointed to "the omission of the images and a specific description of the subjects to demonstrate that they were actually children,"[57] and Mutschelknaus cited *United States v. Syphers* as precedent.[58] In addition, Mutschelknaus moved to suppress the evidence[59] on the basis that the sixty days granted to the government for the search

51. 564 F. Supp. 2d 1072 (D.N.D. 2008).
52. *Id.* at 1074.
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.* at 1075 (citing United States v. Syphers, 426 F.3d 461, 465 (1st Cir. 2005) (explaining that a "court reviewing a warrant application to search for pornographic materials ordinarily is unable to perform the evaluation required by the Fourth Amendment if the application is based on allegedly pornographic images neither appended to, nor described in, the supporting affidavit.")).
59. *Id.* at 1074.

violated Rule 41(e)(2)(a) of the Federal Rules of Criminal Procedure, which require warrants be executed within ten days.[60]

The district court held that probable cause existed for the issuance of the search warrant of the Mandan residence and the electronic media therein.[61] The court declined to require that images of child pornography, or detailed descriptions of the images, be included with the search warrant application.[62] With regard to Mutschelknaus' argument that the execution of the warrant illegally exceeded the ten days provided for in Rule 41(e)(2)(A), the court quoted *United States v. Hernandez*, which held that "[n]either Fed.R.Crim.P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."[63] Ultimately finding that the sixty days authorized by the issuing magistrate was a reasonable time frame in which the government could search the electronic media devices, the court denied both of Mutschelknaus' motions to suppress.[64]

In 2010, the 8th Circuit Court of Appeals reviewed the district court's ruling denying Mutschelknaus' motions to suppress. After finding that the warrant application contained sufficiently detailed descriptions of the images and after noting the investigator's experience with child pornography cases, the court rejected Mutschelknaus' argument claiming a lack of probable cause.[65] The court then reviewed Mutschelknaus' second argument, that the sixty-day extension the magistrate allowed for forensic analysis of the computer violated Rule 41, and wrote: "Regardless of whether Rule 41 was violated . . . 'noncompliance with Rule 41 does not automatically require exclusion of evidence in a federal prosecution. Instead, exclusion is required only if a defendant is prejudiced or if reckless disregard of proper procedure is evident.'"[66] The court noted that Mutschelknaus did not argue that he was prejudiced by the sixty-day extension, and it reasoned that the nature of electronically stored evidence may cause delays.[67] Finally, the court concluded that the officers did not act with a reckless disregard of proper procedures, and ultimately affirmed the district court's rulings.[68]

60. Fed. R. Crim. P. 41(e)(2)(A).
61. *Mutschelknaus,* 564 F. Supp. 2d at 1076.
62. *Id*.
63. *Id*. (quoting United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002)).
64. *Id*. at 1077.
65. United States v. Mutschelknaus, 592 F.3d 826, 828 (8th Cir. 2010).
66. *Id*. at 829-30 (quoting United States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006)).
67. *Id*. at 830.
68. *Id*.

2. United States v. Cartier

In *United States v. Cartier*,[69] the Spanish Guardia Civil Computer Crime Unit (SGCCCU), working with a private company, developed a software program capable of searching peer-to-peer (P2P)[70] computer networks for child pornography using hash values.[71] During this process, the SGCCCU found that "several of the digital images known to be child pornography were downloaded by an ISP address associated with a computer in North Dakota," and SGCCCU contacted the Federal Bureau of Investigations (FBI).[72] Using the information provided by the SGCCCU, the FBI sought a warrant for Cartier's home, where "agents seized 13 hard drives, two thumb drives, and hundreds of compact discs and video tapes. Over 1,000,000 still images of child pornography and more than 4,000 video images of child pornography were found on the computer seized from Cartier's residence."[73]

On appeal, Cartier claimed the agent failed to establish the probable cause necessary for the warrant since the agent relied on hash values of digital files that the agent did not view.[74] Cartier also argued that the search was overly broad, the warrant did not communicate a search strategy, and that he was not given proper Miranda warnings.[75] In arguing the lack of probable cause, Cartier offered an expert witness who testified that it would be possible for two digital files to have colliding, or overlapping, hash values.[76] The government's expert witness testified that "no two dissimilar files will have the same hash value."[77] The district court sided with the government's expert, and the 8th Circuit Court of Appeals found no factual error in that decision.[78]

In arguing that the search was overbroad, Cartier pointed to the absence of a search strategy, and Cartier offered that, without one, the warrant was

69. 543 F.3d 442 (8th Cir. 2008).

70. "P2P networks allow computers to share files with each other without using a central file server. Instead, every computer connected to the P2P network can send and receive files because each computer acts as both a server and a client. Therefore, each computer that is logged into the P2P network can share information and obtain information from any other computer that is part of the P2P network." *Id*. at 444.

71. Hash values act as electronic fingerprints for digital images. Specifically, a hash value represents an image's identity by a string of numbers and letters. In this case, "the 'hash values' were unique sets of 32 numbers and letters that were calculated using a mathematical algorithm that considered certain data contained in individual files." *Id*. at 444 n.3.

72. *Id*. at 445.

73. *Id*.

74. *Id*.

75. *Id*.

76. *Id.* at 446.

77. *Id*.

78. *Id*.

invalid per se.[79] Specifically, Cartier argued that the warrant should have included a strategy that would protect private files having nothing to do with child pornography from the search.[80] This issue had not previously been decided in the 8th Circuit but had been rejected by other circuits.[81] In affirming the district court's denials of Cartier's motions to suppress, the court wrote that:

> Cartier [did] not allege that he was prejudiced by any search of unrelated files nor [did] he allege that any unrelated files were actually searched . . . While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se. Therefore, on the facts of this case, we do not find that the absence of a search methodology or strategy was fatal to the validity of the search warrant.[82]

IV. ELECTRONIC SEARCH DISCUSSIONS

As more people begin to use laptops, smartphones, and the cloud for personal uses, discussions about governmental searches of these devices have grown in popularity. Discussions about electronic searches are ongoing in the media, in academic journals, and in the courthouses. It is important that North Dakota's legal community is sensitive to these discussions as we continue to develop this emerging area of the law.

A. IN THE MEDIA: THE NATIONAL SECURITY AGENCY

One of the most prominent debates in the media is about how the United States can strike an appropriate balance between intelligence gathering and privacy protection. As we know, last summer it was learned that wireless providers were providing the government with call information data pursuant to the ECPA. The President made clear, however, that the providers turned this information over pursuant to court orders. Perhaps in part due to growing national concerns about privacy protection, the President remarked at his year-end press conference that the National Security Agency surveillance program would likely be reformed in

79. *Id*. at 447.

80. *Id*.

81. *Id*. (citing United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1108 (9th Cir. 2008); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007); United States v. Hill, 459 F.3d 966, 977–78 (9th Cir. 2006); United States v. Brooks, 427 F.3d 1246, 1251–52 (10th Cir. 2005)).

82. *Id*. at 447-48.

the near future.[83] Members of North Dakota's legal community should stay tuned to this discussion as our nation's leaders weigh current electronic search and seizure law against the privacy expectations of our citizens.

B. IN ACADEMIC JOURNALS: RETHINKING THE PLAIN VIEW DOCTRINE

Legal scholars have been offering opinions about electronic searches for decades. Likely in anticipation of future Supreme Court review, many law review articles have focused on the implication of the plain view doctrine to on-site searches.[84] In particular, these articles often advocate that the current dragnet approach to on-site electronic searches functions similarly to the general warrants that the Constitution sought to prohibit. In 2005, Orin S. Kerr, an Associate Professor at George Washington University Law School, offered three possible remedies to the problems presented by the plain view doctrine:

> The first approach would narrow the plain view exception based on the circumstances of the search, such as the analyst's subjective intent or the tool used. The second approach would narrow the exception based on the nature of the evidence discovered, permitting the use of some kinds of evidence while blocking others. Both of these proposals seem promising at first, but prove difficult to apply in practice. The third proposal is more draconian: it would abolish the plain view exception in digital evidence cases . . . Eliminating the plain view exception for digital searches is not an ideal solution, and it may not be necessary today. But it may eventually prove the best way to restore the function of the Fourth Amendment in a world of digital evidence.[85]

Professor Kerr acknowledged that elimination of the plain view doctrine might not have been quite necessary in 2005. Perhaps elimination of the plain view doctrine is not necessary in 2014, either; however, the legal community should continue to think about what circumstances may render the exception unjust going forward.

---

83. *See President Obama Holds a News Conference*, THE WHITE HOUSE (Dec. 20, 2013), www.whitehouse.gov/photos-and-video/video/2013/12/20/president-obama-holds-news-conference.

84. *See generally* Kerr, *supra* note 15, at 538; *see also* James T. Stinsman, *Computer Seizures and Searches: Rethinking the Applicability of the Plain View Doctrine*, 83 TEMP. L. REV. 1097 (2011).

85. Kerr, *supra* note 15, at 577.

V. CONCLUSION

In conclusion, searches of electronically stored data are becoming increasingly important due to its increase in popularity both in the general public and in criminal investigations. While many people do not recognize differences in electronic storage locations, the law does. Electronic search issues are of significant future importance in North Dakota, where we have limited precedent and an opportunity to lead the way. Lawyers in North Dakota should take part in the debate about the plain view doctrine's implications in on-site searches. These matters affect us not just as professionals in the criminal justice system, but also as citizens. In addition, Congress or the courts should offer Fourth Amendment protections to remotely stored personal data. While the SCA establishes a current standard for government search, the third-party doctrine established by the Supreme Court's application to this electronic information is uncertain. These typically personal communications, despite often being held by third parties, are deserving of the same protections they would have in our physical homes.

*Quinn Hochhalter**

* 2015 J.D. Candidate from the University of North Dakota School of Law. I would like to thank my family and loved ones for their continued support and guidance. I would also like to thank Jennifer Puhl for inspiring the topic of this note.