2012

Warrantless Cell Phone Searches and the 4th Amendment: You Think You Deleted Those Text Messages … But You Have No Idea …

Amanda Brill
Seton Hall Law

WARRANTLESS CELL PHONE SEARCHES AND THE 4TH AMENDMENT: YOU *THINK* YOU DELETED THOSE TEXT MESSAGES…BUT YOU HAVE NO IDEA…

*****Amanda Brill

I. INTRODUCTION

It seems that with each passing day, a new form of technology is created. Our society is transforming into one reliant on the technology we are constantly introduced to. Computers, cell phones, IPods, and IPads encourage us to rely on electronic pathways to live our daily lives. But while we utilize technology each day, and trust these gadgets to store our most important tasks, appointments, thoughts, and contacts, the law is struggling to keep up.

Cell phones have been a major problem for courts in recent years; more particularly, how to apply the Fourth Amendment when a cell phone is searched by law enforcement officials incident to an arrest. Some courts find that during arrests for routine traffic stops, it is reasonable to search one's cell phone without consent or notice to the cell phone owner. Other courts find the warrant requirement of the Fourth Amendment a necessary element to any search of a cell phone, regardless of the circumstances surrounding the search.

Furthermore, companies such as Cellebrite market "mobile forensic" capabilities which complicate this Fourth Amendment question. Cellebrite boasts "unparalleled access to phone memory" regardless of phone lock codes or deleted items.[1] Cellebrite's CEO Aviad Ofrat told a trade magazine that "mobile device forensics is the future."[2] He further stated that "with the wealth of data even a casual user has stored in his or her cell phone, smart-phone, or PDA, it is quickly becoming THE one piece of evidence that is interrogated immediately."[3] How far should these companies, through law enforcement officers, be allowed to take their intrusions into one's private life? This question has sparked much debate between law enforcement and privacy advocates around the country.

---

[1] CELLEBRITE, http://www.cellebrite.com (last visited Nov. 11, 2011).
[2] Alexis Madrigal, *What Does Your Phone Know About You? More Than You Think*, THE ATLANTIC (Apr. 25, 2011, 10:33 AM), http://www.theatlantic.com/technology/archive/2011/04/what-does-your-phone-know-about-you-more-than-you-think/237786/.
[3] *Id*.

Have our privacy rights disappeared as we store all of our private communications and documents on our cell phones? Does a routine traffic stop allow a law enforcement officer to search and extract data from a cell phone merely because they want to do so? If someone is arrested, is that reason enough to have their cell phone's history, call logs, applications, pictures, messages, e-mails, and videos, among dozens of other personal items, be searched and extracted? All of these privacy concerns have been examined by courts across the country, yet these courts have come to very dissimilar conclusions.

This paper will analyze how courts have addressed warrantless cell phone searches, and then apply this case law to mobile forensic technology to analyze how courts might address the warrantless extraction of cell phone data. Additionally, it will consider where the line should be drawn, if any, when it comes to searching and extracting the contents of a cell phone and further, the emerging issues regarding "cloud computing" and privacy rights.

II. An Overview of the Fourth Amendment

The Fourth Amendment protects citizens against unreasonable searches and seizures. It states that

> 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.[4]

The Supreme Court recognizes that this "security" against unreasonable searches and seizures upon the private lives of people is important and necessary and that "the framers of the Fourth Amendment required adherence to judicial processes wherever possible."[5] The Court has also

[4] U.S. Const. amend. IV.
[5] United States v. Matlock, 415 U.S. 164, 185 (1974) (citing Trupiano v. United States, 334 U.S. 699, 705 (1948)).

stated that "the presence of a search warrant serves a high function."[6] The primary role of the Fourth Amendment is to place a magistrate judge between the citizen and the police and "absent some grave emergency," this system should not be disrupted.[7] Therefore, whenever practicable, and if no exception to the warrant requirement applies, "the police must…obtain advance judicial approval of searches and seizures through the warrant procedure" and "the scope of [a] search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[8]

It is well established law that "the capacity to claim the protection of the Fourth Amendment depends…upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."[9] The Supreme Court has adopted the *Katz* test from Justice Harlan's famous concurrence which explained that there are two parts to any inquiry into whether someone has a legitimate expectation of privacy: first, privacy must be looked at subjectively, meaning someone must have exhibited an actual expectation of privacy, and second, one's expectation of privacy must be "one that society is prepared to recognize as 'reasonable.'"[10]

A. EXCEPTIONS TO THE FOURTH AMENDMENT'S WARRANT REQUIREMENT

Exceptions to the warrant requirement have been named "few in number and carefully delineated,"[11] giving law enforcement the heavy burden of demonstrating "an urgent need that

[6] Groh v. Ramirez, 540 U.S. 551, 557 (2004) (citing McDonald v. United States, 335 U.S. 451, 455 (1948)).
[7] United States v. Morgan, 743 F.2d 1158, 1168 (6th Cir. 1984) (citing *McDonald*, 335 U.S. at 455).
[8] Terry v. Ohio, 392 U.S. 1, 19–20 (1968) (A search undertaken during a "stop and frisk" was found reasonable because it was a protective search for weapons, thus, an acceptable warrantless search under the Fourth Amendment).
[9] Rakas v. Illinois, 439 U.S. 128, 143 (1978).
[10] Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).
[11] United States v. U.S. District Court (*Plamondon*), 407 U.S. 297, 318 (1972).

might justify [a] warrantless search."[12] However, courts have recognized that the "overriding principle of the Fourth Amendment is one of reasonableness," and thus, exceptions to the warrant requirement have been "carved out in a logical and flexible manner."[13]

First and foremost, if a suspect or arrestee voluntarily consents to a search, without any form of police coercion, a warrant is not required.[14] Additionally, the warrant requirement is excused when exigent circumstances are present. Exigent circumstances "excuse an officer from having to obtain a magistrate's determination that probable cause exists; it does not permit a search in the absence of probable cause."[15] These circumstances require immediate action to be undertaken by law enforcement in order to "prevent flight, safeguard the police or public, or to protect against the loss of evidence."[16] In addition to probable cause to search, an officer "must have probable cause to believe that the persons or items to be searched or seized might be gone, or that some other danger would arise, before a warrant could be obtained."[17] The focus becomes whether ""the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment."[18]

Another exception is the "search incident to arrest." The Supreme Court has held that immediately upon arresting an individual, an officer may lawfully search that person without obtaining a warrant.[19] Officers may also search the area within the arrestee's immediate control.[20] These warrantless searches have traditionally been justified by the fact that it is

---

[12] Welsh v. Wisconsin, 466 U.S. 740, 749 (1984).
[13] United States v. Martin, 806 F.2d 204, 206 (8th Cir. 1986).
[14] Schneckloth v. Bustamonte, 412 U.S. 218, 228 (1973) (holding that a search pursuant to consent, properly conducted, is a constitutionally permissible and wholly legitimate aspect of effective police activity).
[15] STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE INVESTIGATIVE: CASES AND COMMENTARY 361 (9th ed. 2010).
[16] *Id*.
[17] *Id*.
[18] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).
[19] United States v. Robinson, 414 U.S. 218 (1973).
[20] Chimel v. California, 395 U.S. 752, 763 (1969).

reasonable for law enforcement to immediately search for weapons, instruments of escape, and evidence of a crime upon an arrest.[21] These have been called "protective searches" since they address the possibility that a weapon may be easily accessible to an arrestee that may put officers at risk, or evidence on or around an arrestee that could be concealed or destroyed. The Court has reasoned that "a gun on a table or in a drawer in front of one who is arrested can be as dangerous to the arresting officer as one concealed in the clothing of the person arrested" and that, therefore, there is "ample justification…for a search of the arrestee's person and the area within his immediate control."[22]

Searches that are incident to arrests and based on probable cause have also included pre-incarceration "inventory searches" which have also been deemed admissible and do not require a warrant under the Fourth Amendment. This is because the lawful arrest itself establishes authority to search, and therefore "a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment."[23] An inventory search must be regulated by "standardized criteria" or "established routine" so as not to "be a ruse for a general rummaging in order to discover incriminating evidence."[24] The search may include containers or articles in an arrestee's possession at the time of arrest.[25] A container is "any object capable of holding another object."[26] Containers include "glove compartments, consoles, or other receptacles located anywhere within [a] passenger compartment, as well as luggage, boxes, bags, clothing, and the

[21] United States v. Edwards, 415 U.S. 800, 802-03 (1974).
[22] *Chimel*, 395 U.S. at 763.
[23] *Robinson*, 414 U.S. at 235.
[24] Florida v. Wells, 495 U.S. 1, 4 (1990).
[25] Illinois v. Lafayette, 462 U.S. 640, 648 (1983).
[26] New York v. Belton, 453 U.S. 454, 460 (1981).

like" and may be searched whether they are open or closed.[27] Such container searches have been permitted not because a suspect has no privacy interests in his personal effects, but because "[a] lawful custodial arrest justifies the infringement of any privacy interest" a suspect may have in such effects.[28]

Another common exception is the "plain view doctrine." In some circumstances, law enforcement officers may seize evidence in plain view without having a warrant.[29] Under *Coolidge*, the plain view doctrine applies when three requirements are met: "(1) the intrusion by the police must have a prior justification under the Fourth Amendment; (2) the discovery of the evidence must be 'inadvertent'; and (3) it must be 'immediately apparent' to the police that the items are evidence or otherwise subject to seizure."[30] The Supreme Court, however, has clarified that "while inadvertence is a characteristic of most legitimate 'plain view' seizures, it is not a necessary condition."[31] Similarly, the "inevitable discovery doctrine" is an exception maintaining that "evidence obtained during the course of an unreasonable search and seizure should not be excluded 'if the government can prove that the evidence would have been obtained inevitably' without the constitutional violation."[32]

The automobile exception to the warrant requirement addresses the warrantless search of an automobile that has been stopped by law enforcement officers who had probable cause to believe that the vehicle contained incriminating evidence.[33] Often it may not be practicable to secure a warrant for the automobile if "the vehicle can be quickly moved out of the locality or

[27] *Id*. *See infra* Part III.A (discussing case law finding cell phones to be containers), and Part IV.C.3 (suggesting the possibility that "electronic containers" could be an exception to the general container rule).
[28] *Id*. at 461.
[29] Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971).
[30] *Martin*, 806 F.2d at 206–07.
[31] Horton v. California, 496 U.S. 128, 130 (1990).
[32] United States v. Heath, 455 F.3d 52, 55 (2d Cir. 2006) (citing Nix v. Williams, 467 U.S. 431, 447 (1984)).
[33] California v. Acevedo, 500 U.S. 565 (1991).

jurisdiction in which the warrant must be sought."[34] The general rule is that "if a car is readily mobile and probable cause exists to believe it contains contraband, the Fourth Amendment…permits police to search the vehicle without more."[35] The Supreme Court has extended this rule by stating that the warrantless search of an automobile could include a "probing search" of a container or package found inside the car when the search is supported by probable cause.[36] Thus, "if probable cause justifies the search of a lawfully stopped vehicle, it justifies the search of every part of the vehicle and its contents that may conceal the object of the search."[37]

B. HOW ADVANCES IN TECHNOLOGY HAVE CHANGED THE FOURTH AMENDMENT

As new technology arises, it changes and enhances the world in which we live, so the law adapts accordingly. The Supreme Court openly acknowledged that "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[38] Today, the advancements in cell phone technology provide law enforcement with a "virtual Rolodex of alleged criminal contacts – something that days of coercion, interrogation or even torture may not reveal."[39] Very quickly, these advanced cell phones are becoming less of a secure and private communication tool, rather, they are more of a "hangman's noose."[40] But should advancements in technology force us to give up our core civil liberties and constitutional rights? Not necessarily. Although the Fourth Amendment has been interpreted to protect a citizen's right of privacy, "the extent to which the Fourth Amendment provides protection for the contents of electronic communications (such as

[34] *Id*. at 569 (quoting Carroll v. United States, 267 U.S. 132, 153 (1923)).
[35] Pennsylvania v. Labron, 518 U.S. 938, 940 (1996).
[36] United States v. Ross, 456 U.S. 798, 800 (1982).
[37] *Id*. at 825.
[38] Kyllo v. United States, 533 U.S. 27, 33-34 (2001)
[39] David Mock, *Wireless Advances the Criminal Enterprise*, THE FEATURE ARCHIVES WEB (June 28, 2002), http://thefeaturearchives.com/topic/Technology/Wireless_Advances_the_Criminal_Enterprise.html.
[40] *Id*.

images stored on a cell phone)…is an open question."[41] The way courts interpret the Fourth Amendment will ultimately give us guidance into how protected we are with respect to the information stored in cell phones.

1. APPLICATION OF THE FOURTH AMENDMENT TO CELL PHONES

Today, cell phones are used for countless reasons by millions of people.[42] Advances in cell phone technology have equipped users with portable personal computers, allowing people to store everything they need to live their daily lives on a handheld device. The potential information stored on cell phones includes items such as "subscriber and equipment identifiers; phonebook information; appointment calendars; text messages; call logs for dialed, incoming, and missed calls; email; photographs; audio and video recordings; multimedia messages; instant messaging; Web browsing history; electronic documents; and user location information."[43]

No longer do cell phones merely place calls without a landline connection; cell phones have become very "smart." A "smartphone" is "a cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system, Web browsing and the ability to run software applications" along with "texting, gaming, personal information management and cameras."[44] Smartphones provide advanced computing and have the capability to run mobile applications with more connectivity, processing, and storage options

[41] Newhard v. Borders, 649 F. Supp. 2d 440, 448 (W.D. Va. 2009).
[42] "As of June 2010, there were approximately 292.8 million U.S. cell phone users." Ashley B. Snyder, Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 162 (2011).
[43] *Id*. at 162-63.
[44] *Smartphone*, SEARCH MOBILE COMPUTING, http://searchmobilecomputing.techtarget.com/definition/smartphone (last updated Aug. 2000).

than regular cell phones.[45] A smartphone is "a social network and entertainment center all rolled into a solitary, convenient device."[46]

With the vast amount of information accessible from a cell phone, privacy issues would necessarily transpire. It is obvious why law enforcement officers would want to search a cell phone's content in the hopes they might find something incriminating to use later against the arrestee-cell phone owner. Courts in turn must maintain the privacy every citizen expects in their handheld technology to the extent it is reasonable in each arrest situation. "Smartphones make up a growing share of the United States mobile phones market, and are likely to be pervasive in the near future…The question of when and how they may be searched is therefore an important one."[47]

2. Do People Have a Reasonable Expectation of Privacy in Their Cell Phones?

Courts have come to varied conclusions as to whether the *Katz* test has been satisfied so as to provide a reasonable expectation of privacy to a cell phone user in their device.[48] The background case law on telephone landlines marks the beginning of this discussion. In the 1979 Supreme Court case *Smith v. Maryland*, police officers, without a warrant, installed a pen register in a telephone system to intercept calls coming into a robbery victim's home in order to establish who and where the calls were coming from.[49] Once the defendant was identified as the caller, the Court held that the defendant did not have an expectation of privacy in the numbers that he dialed from his phone since those numbers were automatically turned over to a third

---

[45] David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Forensic Focus: Articles/Papers (Aug. 20, 2011), http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/.
[46] *Id*.
[47] People v. Diaz, 244 P.3d 501, 514 (Cal. 2011) (Werdegar, J., dissenting).
[48] *See* cases cited *supra* note 10 for a discussion of the *Katz* test.
[49] *Smith*, 442 U.S. at 737.

party, the phone company.[50] The Court also stated that even if the defendant did have some subjective expectation of privacy in the numbers he dialed, this was not an expectation that society was prepared to recognize as reasonable.[51] Therefore, the Court ultimately held that the installation of the pen register to recover telephone numbers dialed by the defendant was not a "search" under the Fourth Amendment, and no warrant was required.

While *Smith* was decided before cell phones were in use, the same issue the Supreme Court addressed back in 1979 is called into question now: if a cell phone user has provided information to third parties like Verizon and AT&T, do they have an expectation of privacy in their call logs? Courts today generally conclude that the content and information a person stores on his or her cell phone, like one's call log, is entitled to some form of privacy.[52] In order to obtain this information, most courts agree that a warrant is required, unless an exception to the warrant requirement applies. Many courts have found that a person has a reasonable expectation of privacy in their cell phone when they claim to have a possessory interest, a right to control access, or show some sort of subjective expectation of privacy, for example, by taking precautionary measures to maintain the expected privacy like locking the phone or keeping it on his or her person.[53]

---

[50] *Id*. at 742-44.
[51] *Id*. at 743.
[52] *See, e.g.*, State v. Boyd, 992 A.2d 1071, 1082 (Conn. 2010) (individual has a reasonable expectation of privacy in all of the contents of his cell phone, including his subscriber number); United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (individual has reasonable expectation of privacy in information contained in cell phone because they contain a wealth of private information); United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2008) ("An owner of a cell phone generally has a reasonable expectation of privacy in the electronic data stored on the phone."); United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1139 (D.N.M. 2004) (There is "an expectation of privacy in an electronic repository for personal data, including cell telephones."); United States v. James, No. 1:06CR134, U.S. Dist. LEXIS 34864, at *10 (E.D. Mo. Apr. 29, 2008) ("It is reasonable for a person to expect the information contained in a cell phone—especially information such as that contained in the address book, which is not available even to the service provider—will be free from intrusion from both the government and the general public."). *But see* United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1276 (D. Kan. 2007) (Defendant did not assert ownership to the phones, nor did he present any evidence that they were his or insure his privacy in them, so the court found that he had no reasonable expectation of privacy in the content of the phones).
[53] *See* State v. Sealy, 546 A.2d 271, 273 (Conn. 1988); United States v. Finley, 477 F.3d 250, 259 (5th Cir. 1997).

III. The Split of Authority Regarding Warrantless Searches of Cell Phones

There is a split of authority, in both federal and state courts, regarding whether a warrant is required to search a cell phone or retrieve information on a cell phone pursuant to an arrest. The case law on this subject analyzes whether the search of the phone is legitimate and, for the purposes of this paper, provides a framework for analyzing the constitutionality of using extraction technology.

A. Cases that Find Searches of a Cell Phone Without a Warrant Reasonable

Courts that find warrantless cell phone searches reasonable generally follow the search incident to arrest exception or the exigency exception to the Fourth Amendment. Searches have been deemed necessary to prevent the destruction of evidence when incoming calls or text messages override previous ones, or have been justified as inventory searches. Cell phones have also been compared to pagers, which most courts have found to be searchable without a warrant. Courts also maintain that the type of information stored on one's cell phone is similar to that which is found in a wallet or address book, both of which have been found to be searchable incident to arrest.[54]

1. Federal Law Permitting Warrantless Searches

In 2009, the Fourth Circuit in *United States v. Murphy* upheld a warrantless search of an arrestee's cell phone under the search incident to arrest exception.[55] In this case, after the officers had arrested the defendant for obstruction of justice for giving them false names, the officers searched the defendant's phone to uncover possible incriminating evidence about the

[54] United States v. Cote, No. 03CR271, 2005 U.S. Dist. LEXIS 11725, at *6 (N.D. Ill. May 26, 2005) ("Searches of items such as wallets and address books, which [the court] consider[ed] analogous to [Defendant's] cellular phone since they would contain similar information, have long been held valid when made incident to an arrest."), *aff'd*, 504 F.3d 682 (7th Cir. 2007).

[55] United States v. Murphy, 552 F.3d 405, 411 (4th Cir.) *cert. denied*, 129 S. Ct. 2016 (2009).

defendant regarding drug activity and the existence of counterfeit money.[56] The search of the phone occurred multiple times; once in the defendant's presence and again at the police department.[57] The searches ultimately uncovered text messages that were determined to be sent from the defendant's drug dealer.[58] The court found that the searches of the defendant's phone were acceptable without a warrant because the first search was a search incident to defendant's lawful arrest, and the second search was a valid inventory search which was also necessary to preserve evidence stored on the phone.[59] The court determined that "officers may retrieve text messages and other information from cell phones and pagers seized incident to an arrest" for the purpose of preservation since call logs and text messages may be overwritten as new calls and text messages are received.[60]

Similarly, the Fifth Circuit, in *United States v. Finley*, found that the law enforcement officer's warrantless cell phone search of the defendant's call log and text messages was proper as incident to a lawful arrest.[61] The defendant in *Finley* was arrested on drug charges and, incident to his arrest, he was searched and his phone was seized.[62] Although the officers transported the defendant to the accomplice's home and later searched the cell phone outside the home, after the defendant had already been taken into custody, the search was still "substantially contemporaneous with his arrest."[63] The court justified the search as permissible by characterizing the phone as a container, and therefore, searchable upon the defendant's lawful

[56] *Id*. at 409.
[57] *Id*. at 412.
[58] *Id*. at 409.
[59] *Id*. at 412.
[60] *Id*.
[61] United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007); *accord* United States v. Curtis, 635 F.3d 704, 712 (5th Cir. 2011).
[62] *Finley*, 477 F.3d at 253.
[63] *Id*. at 260.

arrest.[64] The court decided that "police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial."[65] In *United States v. Curtis*, the Fifth Circuit affirmed a denial of the defendant's motion to suppress text messages taken on his phone pursuant to the *Finley* rule of authorizing police officers to search the electronic contents of an arrestee's cell phone recovered from the area within said arrestee's immediate control.[66]

The Seventh Circuit, in *United States v. Ortiz*, also followed the search incident to arrest exception when addressing the issue of a warrantless search.[67] While this case concerned a pager, a pager is very similar to a cell phone in that it stores personal information and data, and there is an identical necessity to preserve evidence in pagers as there is in cell phones as discussed in *Murphy*.[68] In *Ortiz*, the court held that law enforcement officers may search or retrieve information from a pager in order to prevent its destruction as evidence.[69] The court maintained that "an officer's need to preserve evidence is an important law enforcement component of the rationale for permitting a search of a suspect incident to a valid arrest."[70] Further, due to the "finite nature of a pager's electronic memory, incoming pages may destroy currently stored telephone numbers in a pager's memory."[71]

---

[64] *Id.*
[65] *Id.*
[66] United States v. Curtis, 635 F.3d 704, 711-14 (5th Cir. 2011).
[67] United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996); *see also* United States v. Pineda-Areola, 372 F. App'x 661, 662 (7th Cir. 2010); *accord* Silvan W. v. Briggs, 309 F. App'x 216, 225 (10th Cir. 2009).
[68] *Murphy*, 552 F.3d at 412. *See also* United States v. Young, 278 F. App'x 242, 245-46 (4th Cir. 2008) (per curiam) (noting that the Fourth Circuit had previously found pagers to be searchable incident to arrest, and extending this reasoning to justify the search incident to arrest of a cell phone's text messages).
[69] *Ortiz*, 84 F.3d at 984.
[70] *Id.*
[71] *Id.*

The District Court of Minnesota followed *Finley* and *Ortiz* in deciding that if a cell phone is lawfully seized, officers may also search any data electronically stored in the device."[72] In this case, after arresting one of two defendants for drug distribution and conspiracy, the officers searched the "electronic memory" of his two cell phones for information linking both the two defendants and their criminal acts."[73] Further, the District Court of Arizona decided a case where a defendant was arrested for drug-trafficking and law enforcement agents searched the phone only minutes after the arrest and later seized the phone for the purpose of uncovering his call log.[74] Based upon the fact that the agents were in a desperate need to find other suspects who were at large, as well as the good reason they had to believe that the other suspects were in contact with the defendant through his cell phone, the court found this search permissible as a search incident to an arrest.[75] Additionally, the court noted that "there is authority for the proposition that cell phones…in drug-trafficking investigations may come within the plain view exception to the warrant requirement as items akin to contraband, in that they are often tools of the drug-trafficking trade."[76]

The District Court of Kansas rejected the defendant's motion to suppress evidence seized from his cell phone pursuant to a warrantless search.[77] The officers searched the cell phone after the defendant was arrested for various drug charges, and the court found that the search was properly within the scope of an inventory search pursuant to a search incident to arrest.[78] A question remained, however, whether the officer in this case was acting unreasonably when

---

[72] United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008).
[73] *Id*.
[74] United States v. Santillan, 571 F. Supp. 2d 1093, 1102 (D. Ariz. 2008).
[75] *Id*.
[76] *Id*. *See also* United States v. Martinez, 938 F.2d 1078, 1083-84 (10th Cir. 1991); *Morales-Ortiz*, 376 F. Supp. 2d at 1141.
[77] United States v. Parada, 289 F. Supp. 2d 1291, 1303 (D. Kan. 2003).
[78] *Id*.

noting the numbers of incoming calls that the phone was receiving and storing in its memory.[79] The court concluded that "because a cell phone has a limited memory to store numbers" the officer acted reasonably when he recorded the numbers "in the event that subsequent incoming calls effected the deletion or overwriting of the earlier stored numbers."[80] Ultimately, as a matter of exigency, the court held that the officer had "the authority to immediately search or retrieve the cell phone's memory of stored numbers of incoming calls in order to prevent the destruction of this evidence."[81]

2. State Law Permitting Warrantless Searches

This year, in *People v. Diaz*, the Supreme Court of California determined that the search of the defendant's cell phone text message folder, which occurred at the police station, was valid without a warrant.[82] The defendant was arrested for being a coconspirator in the sale of drugs, and his cell phone was located on his person.[83] The issue became whether it was unreasonable that the search of the cell phone was delayed until after the defendant was taken into custody.[84] If the court determined that the cell phone was "immediately associated with [his] person," then the delayed warrantless search was valid incident to his lawful arrest, but if it was not, then the search was invalid as being too "remote in time and place from the arrest" unless an exigency applied.[85] The court ultimately held the search to be valid because the cell phone "was an item [of personal property] on [defendant's] person at the time of his arrest and during the administrative processing at the police station."[86] The court analogized the cell phone to an article of clothing found on a person, just as the phone was found on the defendant and in his

[79] *Id.*
[80] *Id.*
[81] *Id.* at 1304.
[82] People v. Diaz, 244 P.3d 501, 502 (Cal. 2011).
[83] *Id.*
[84] *Id.* at 505.
[85] *Id.* (citing United States v. Chadwick, 433 U.S. 1, 15 (1977)).
[86] *Diaz*, 244 P.3d at 505.

immediate control.[87] Although the court found no exigent circumstances apparent to otherwise justify the warrantless search, the immediate association of the cell phone with the defendant after the arrest was enough to justify the police inspection at the station without a warrant.[88]

A Florida appellate court also upheld the warrantless search of a cell phone when a police officer searched the defendant's cell phone pursuant to his arrest for sexual battery of a child.[89] When the officer first took possession of the phone from the defendant's pocket, the defendant became very nervous, causing the officer to flip open the phone to ensure that it was not a disguised weapon.[90] Upon opening the phone, the officer noticed that the wallpaper behind the phone's main menu was a picture of a prepubescent female in a sexually compromised position.[91] Based upon the nature of the defendant's arrest, the officer decided to search the media files on the cell phone, further uncovering images of child pornography.[92] The court followed *Finley* and concluded that the phone was a container and searchable under the search incident to arrest exception.[93] It stated that "digital files and programs on cell phones have merely served as replacements for personal effects like address books, calendar books, photo albums, and file folders previously carried in a tangible form."[94] Further, when viewed in this light, the phone was merely a case, a closed container, containing these personal effects.[95]

A Georgia appellate court upheld a warrantless cell phone search of the defendant's phone following her arrest for unlawfully attempting to purchase a controlled substance.[96] The officer had been using the alleged drug dealer's cell phone to communicate with the defendant

---

[87] *Id*.
[88] *Id*.
[89] Fawdry v. State, 70 So. 3d 626, 627 (Fla. Dist. Ct. App. 2011).
[90] *Id*.
[91] *Id*.
[92] *Id*. at 628.
[93] *Id*. at 630.
[94] *Id*.
[95] *Id*.
[96] Hawkins v. State, 704 S.E.2d 886, 888 (Ga. Ct. App. 2010).

and ultimately plan a meeting for her to make a buy.[97] At the designated meeting spot, the officer observed the defendant in her car "entering data into her phone" and the officer "almost contemporaneously received another text message" announcing her arrival at the meeting place.[98] The officer approached the defendant's car, identified himself, and arrested her.[99] With the defendant's consent, and as a search incident to her arrest, the officer searched the defendant's vehicle and uncovered her cell phone inside her purse.[100] The officer searched the phone for the text messages regarding the drug sale and, to preserve the messages, the officer downloaded and printed them.[101] The court determined that "when an officer is authorized to search in a vehicle for a specific object and…comes across a container that reasonably might contain the object of his search," namely, the cell phone, "the officer is authorized to open the container and search within it for the object."[102] Accordingly, the court held that the cell phone was enough like a container to be treated like one "in the context of a search for electronic data," and the officer, believing that he would find what he was seeking on the phone, was therefore within reason when he searched its contents.[103]

B. CASES THAT FIND SEARCHES OF A CELL PHONE WITHOUT A WARRANT UNREASONABLE

Other federal and state courts have chosen to prohibit warrantless cell phone searches entirely. These courts generally rely on the principle that no exigency or need for officer safety exists, or that a delay between the arrest and the search was unreasonable. Further, these courts recognize that the immense amount of personal data stored on cell phones generates a greater expectation of privacy, and thus, justifies heightened protection under the Fourth Amendment.

---

[97] *Id*.
[98] *Id*.
[99] *Id*.
[100] *Id*.
[101] *Id*.
[102] *Id*. at 889.
[103] *Id*. at 890.

1. FEDERAL LAW PROHIBITING WARRANTLESS SEARCHES

The District Court of Nebraska concluded that the warrantless search of defendant's cell phone was unreasonable.[104] The defendant was arrested in 2009 for distributing and conspiring to distribute crack cocaine in 2008.[105] During a search pursuant to his arrest, a cell phone was obtained from the defendant and the officer scanned and saved the contact list on the phone.[106] The court concluded that this search was unjustified because the officer could not reasonably believe that searching the phone would uncover evidence of a crime that allegedly occurred a year earlier.[107] Further, "the phone did not present a risk of harm to officers or appear to be contraband or destructible evidence."[108] The court determined that the search was an invalid search incident to arrest.[109]

The District Court for the Northern District of California granted a motion to suppress the warrantless search of the defendants' cell phones.[110] The defendants in this case were arrested for conducting a drug operation inside a residence.[111] At the time of their arrests, no officer searched or seized any of the defendants' cell phones.[112] Once at the station, the cell phones' address books and memory were searched by the officers.[113] The court held that the officers did not successfully point to any exception to the warrant requirement to justify the searches and that the searches were "purely investigatory."[114] Since the search of the phones occurred more than an hour and a half after the arrest, it went "far beyond the original rationales for searches incident

---

[104] United States v. McGhee, No. 8:09CR31, 2009 U.S. Dist. LEXIS 62427, at *3 (D. Neb. July 21, 2009).
[105] *Id.* at *1.
[106] *Id.* at *2.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] United States v. Park, No. CR 05-375 SI, 2007 U.S. Dist. LEXIS 40596, at *2 (N.D. Cal. May 23, 2007).
[111] *Id.* at *3.
[112] *Id.*
[113] *Id.* at *8.
[114] *Id.* at *24.

to arrest, which were to remove weapons to ensure the safety of officers and bystanders, and the need to prevent concealment or destruction of evidence."[115] The court also noted that since cell phones "have the capacity for storing immense amounts of private information," they are similar to computers, in which arrestees have significant privacy interests, rather than address books or pagers found on one's person, in which one's privacy interest decreases.[116]

The District Court of Hawaii granted a motion to suppress all of the evidence obtained from the defendant's cell phone during a search that was not determined to be contemporaneous with the defendant's arrest.[117] In this case, the defendant was arrested for being involved with drug smuggling and two cell phones were taken from him upon arrest.[118] At the station, while the defendant was being processed, an officer searched the phones under the belief that they might contain evidence of a crime.[119] One of the phones was unlocked and the officer was able to observe the defendant's recent calls, text messages, and address book.[120] The court determined, however, that the time period between the arrest and the search "spanned somewhere between two hours and fifteen minutes to three hours and forty-five minutes," and the arrest and search also took place miles apart from each other.[121] The government did not provide any legitimate excuse for the delay, and therefore, judging from the time period and physical distance between the arrest and search, the court held that the search was not "at about the same time of the arrest" or "roughly contemporaneous" with the arrest.[122]

---

[115] *Id*. *Accord Quintana*, 594 F. Supp. 2d at 1301 (holding that contents found on defendant's cell phone should be suppressed as the search of the phone's contents had "nothing to do with officer safety or the preservation of evidence related to the crime of arrest").
[116] *Park*, 2007 U.S. Dist. LEXIS 40596, at *24.
[117] United States v. Lasalle, No. 07-00032, 2007 U.S. Dist. LEXIS 34233, at *1 (D. Haw. May 9, 2007).
[118] *Id*. at *5.
[119] *Id*. at *7.
[120] *Id*.
[121] *Id*. at *19.
[122] *Id*. (citing United States v. McLaughlin, 170 F.3d 889, 892 (9th Cir. 1999) and United States v. Turner, 926 F.2d 883, 887 (9th Cir. 1991)).

2. STATE LAW PROHIBITING WARRANTLESS SEARCHES

The Ohio Supreme Court, in *State v. Smith*, was the first high court in the country to consider the topic of a warrantless cell phone search incident to arrest.[123] In this case, the defendant was arrested for selling drugs and officers searched his cell phone for call records and phone numbers that could further prove the defendant's job as a drug dealer.[124] While the state wanted the court to characterize the cell phone as a closed container like in *Finley*, the court refused.[125] Instead, the court reasoned, as the U.S. Supreme Court has, that "objects falling under the banner of 'closed container' have traditionally been physical objects capable of holding other physical objects," which a cell phone is not.[126] The court acknowledged that, while in the past, electronic devices such as pagers were found to be closed containers subject to search, these cases never considered the U.S. Supreme Court's definition of container "which implies that the container must actually have a *physical* object within it."[127] Due to the modern cell phone's ability to store "a wealth of *digitized* information wholly unlike any physical object found within a closed container" it could not be considered "a closed container for the purpose of a Fourth Amendment analysis."[128] Additionally, the court also found that there was no evidence that the search of the phone's content was necessary to ensure the officer's safety or to prevent imminent destruction of the information.[129] Thus, the court held that the cell phone search was unreasonable and intrusive and a warrant should have been secured.

IV. MOBILE FORENSIC TECHNOLOGY USED IN THE EXTRACTION OF CELL PHONE INFORMATION

---

[123] State v. Smith, 920 N.E.2d 949, 950 (Ohio 2009).
[124] *Id.*
[125] *Id.* at 953.
[126] *Id. See also Belton*, 453 U.S. at 460 (discussing containers).
[127] *Smith*, 920 N.E.2d at 954 (emphases added).
[128] *Id.* at 955 (emphasis added).
[129] *Id.*

The constitutionality of warrantless cell phone searches has been considered for more than a decade. Rick Mislan, an assistant professor of computer and information technology at Purdue University, stated that "cell phones are ubiquitous in today's world and nearly all crimes have a digital component to them."[130] As the number of cell phone users, as well as the types of cell phones available with unlimited abilities, increases, it is reasonable to see why law enforcement desires the ability to flip through a person's phone to uncover incriminating information. Now, officers can not only flip through a phone, but they can also extract the content of the phone.[131] Before extraction technology became available, law enforcement agencies were no doubt at a disadvantage to criminals.[132] Tracking and extraction devices, with the help of mobile device forensics, are becoming increasingly available to assist law enforcement in obtaining information on cell phones. However the extraction process can prove to be very difficult due to the "volatile nature of electronic evidence."[133]

Cell phone users are generally innocent as "most cell phone owners think simply removing a phone's SIM card removes personal information, but the phone's internal memory, even communication exchanged between the phone and its server, remain."[134] It is mobile forensic technology that makes all of the so called deleted information retrievable again. Everyday users "continue to pump ever more data into cell phones . . . those indispensable companions that have so much to say about us."[135] Yet mobile forensics continue to expand in

[130] Hilary Hylton/Austin, *What Your Cell Knows About You*, TIME (Aug. 15, 2007), http://www.time.com/time/health/article/0,8599,1653267,00.html.
[131] *See infra* Part IV.A (discussing extraction technology).
[132] Hylton/Austin, *supra* note 127.
[133] Bennett, *supra* note 44.
[134] Hylton/Austin, *supra* note 127.
[135] *Id*.

nature, and are ultimately able to "get a fingerprint of who [a] person really is" via the information taken off of their cell phone.[136]

A. WHAT IS MOBILE FORENSIC TECHNOLOGY?

Mobile device forensics entails "recovering digital evidence from a mobile device under forensically sound conditions."[137] "Forensically sound" means using "a particular technology or methodology."[138] The need for mobile device forensics was created by "the use of mobile phones in online transactions such as stock trading, flight reservations and check-in; mobile banking; and communications regarding illegal activities that are being utilized by criminals."[139]

Mobile forensic software tools access a wide range of devices to handle "the most common investigative situations with modest skill level requirements" while keeping the device intact.[140] Some situations are more difficult, such as recovering deleted information, and require specialized tools and expertise, and perhaps even the disassembling of the cell phone itself.[141] The most important characteristic of forensic tools is the "ability to maintain the integrity of the original data source being acquired and also that of the extracted data."[142]

The forensic investigator completing the data extraction has one priority, that is, to use the most acceptable methods of obtaining evidence so that the evidence will be admitted accordingly and in an acceptable manner at trial.[143] The evidence will usually be admitted if the trial judge finds that the search was lawful and that "the chain of custody rules including

---

[136] *Id*.
[137] Bennett, *supra* note 44.
[138] *Id*.
[139] *Id*.
[140] WAYNE JANSEN & RICK AYERS, NAT'L INST. OF STANDARDS AND TECH., GUIDELINES ON CELL PHONE FORENSICS 56 (2007), http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.
[141] *Id*.
[142] *Id*.
[143] Bennett, *supra* note 44. While a comprehensive analysis of the authentication and admissibility of the extracted data is beyond the scope of this paper, it is likely to be an issue addressed in the future by forensic investigators, law enforcement officers, and courts alike.

evidence collection, evidence preservation, analysis, and reporting" were adhered to.[144] The International Organization on Computer Evidence has published general principles that are to be followed when recovering digital evidence for chain of custody:

> 1. All of the general forensic and procedural principles should be adhered to when dealing with digital evidence.
> 2. Upon seizing digital evidence, any actions taken should not modify the original evidence.
> 3. When it is necessary for personnel to access the original digital evidence, the personnel should be appropriately trained for the purpose.
> 4. All activities associated to the seizure, access, storage or transfer of digital evidence must be fully and properly documented, preserved and available for review.
> 5. An individual is responsible for all actions taken with respect to digital evidence when digital evidence is in that individual's possession.
> 6. Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with all six principles.[145]

Because of the advancements in cell phones and smartphones, forensic investigation techniques used to recover information have become highly complex and numerous companies in the mobile forensic field boast the capability of obtaining the information law enforcement desires.

B. CELLEBRITE

Cellebrite has been used for over a decade, and "provides the widest coverage in the [mobile forensics] market."[146] Its technology continues to be the most popular of all the mobile forensic technologies. The Cellebrite Universal Forensics Extraction Device (UFED) Forensic System is a device used in the field and the research lab.[147] It supports "most cellular device interfaces…and can provide data extraction of content such as audio, video, phone call history and deleted text messages stored in mobile phones."[148] Cellebrite's UFED System works with

---

[144] *Id*.
[145] *Id*.
[146] *Cellebrite Universal Forensics Extraction Device (UFED)*, CELLEBRITE, http://www.cellebrite.com/forensic-products/forensic-products.html?loc=seg (last visited Nov. 11, 2011).
[147] Bennett, *supra* note 44.
[148] *Id*.

Apple's iPhone, as well as over 3,000 phones by "suck[ing] data out…without the need for an intermediary computer."[149] Cellebrite maintains that it is the "tool of choice for thousands of forensic specialists in police, special forces, tax fraud, customs, border control, and anti-terrorist investigations in more than 60 countries."[150] Cellebrite calls its technology easy to use because UFED gathers its retrieved data into reports for research and evidence which can later be admitted in court.[151]

Cellebrite's tools are made to "dump the entirety of your phone…all of your text messages, emails, videos, and photos – even the ones you deleted – Google Map queries…web searches, passwords, call logs…your phone's entire file system."[152] This information is "all timestamped, all geotagged, all providing a digital recreation of the way your physical existence projects itself into the cellular ether."[153] Cellebrite's website maintains that "for law enforcement, leveraging this valuable resource of information with Cellebrite's UFED System ensures that you get every bit of information necessary to more effectively reach your crime solving goals."[154]

Besides Cellebrite, which claims to have sold 3,500 devices in the eleven months since its UFED System reached the market, other devices are commonly sold and used by law enforcement.[155] Paraben Corporation, Micro Systemation, Susteen, Compelson Labs, Radio

---

[149] Sam Biddle, *The Handheld Dracula That Sucks Your Entire Life From Your Phone*, GIZMODO (Apr. 25, 2011) http://gizmodo.com/5795369/the-handheld-dracula-that-sucks-your-entire-life-from-your-phone.
[150] *Mobile Forensic Customers*, CELLEBRITE, http://www.cellebrite.com/about-us-forensics/customers.html (last visited Nov. 11, 2011).
[151] *Mobile Forensic Solutions for Law Enforcement*, CELLEBRITE, http://www.cellebrite.com/forensic-products/mobile-forensic-solutions/law-enforcement.html (last visited Nov. 11, 2011).
[152] Biddle, *supra* note 145.
[153] *Id*.
[154] *Mobile Forensic Solutions for Law Enforcement*, *supra* note 147.
[155] Madrigal, *supra* note 2.

Tactics, Final Data, Oxygen Software, and Katana Forensics, the makers of Lantern,[156] are other companies which sell devices for cell phone extraction.

C. The Constitutionality of Warrantless Extraction of Cell Phone Data

There are many legitimate pros and cons for needing a warrant to search ones cell phone, and further, to extract the data from the phone itself. As a threshold issue, it must be determined whether extracted data from one's phone, by the use of mobile forensic technology such as Cellebrite, is a search or seizure that would be subject to the Fourth Amendment requirements. A search occurs when "an expectation of privacy that society is prepared to consider reasonable is infringed."[157] The seizure of property occurs when "there is some meaningful interference with an individual's possessory interest in that property."[158] This determination should be considered in light of where the extraction takes place. Additionally, whether a cell phone can be characterized as a container will further determine the constitutionality of using mobile forensic technology to extract data from cell phones.

1. If the Extraction Technology is Being Used in a Lab Setting

If a law enforcement officer has arrested a suspect and desires to search their phone, it may be necessary to take the phone to a lab so that the extraction could be conducted in forensically sound conditions. In this case, it would seem obvious that the phone has been seized in order to take it to an off-site location to extract the data. The Fourth Amendment is thus implicated, and unless an exception to the warrant requirement applies, a warrant would be necessary to search and extract the phone.

---

[156] Lantern, in particular, is an application that one opens on one's cell phone which then essentially creates a time line combining every single communication ever recorded on the phone, as well as pictures, maps, and contacts on one interface. *See Lantern v2.0*, KATANA, http://katanaforensics.com/?page_id=1218 (last visited Nov. 15, 2011).
[157] United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[158] *Id*.

If the phone is taken to a lab, there is significant time between when the phone is taken and when it is connected to a program that will extract its information. Therefore, in the context of a warrantless search and seizure, law enforcement cannot rely on the fact that emergency discounts the need for a warrant, or that any exigency exception could apply. Regardless of how long it takes for an officer to reach a lab from the scene of an arrest, it is reasonable to assume that the officer could obtain a warrant in the proper way, either in person or electronically. Additionally, an officer cannot claim that there is a risk that evidence will be destroyed, concealed, or overridden. Mobile forensic technology prides itself on the ability to obtain information that has been deleted or hidden on a phone. As in *Murphy*, preservation of evidence is no longer necessary as companies like Cellebrite can "dump the entirety" of a person's phone, deleted information and all.[159]

The Supreme Court has held that when an officer makes an arrest, it is reasonable to search the person arrested in order to "remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape."[160] The Court said that "otherwise, the officer's safety might well be endangered, and the arrest itself frustrated."[161] First and foremost, a cell phone is not a gun. It is not dangerous, and it can pose minimal, if any, immediate threat to an arresting officer. By arresting a suspect and removing a cell phone, especially if the phone is removed for the purposes of taking it to an off-site lab for extraction, an officer cannot be considered to be in any danger, nor can the cell phone be used in any way to effect an escape by, perhaps, a suspect calling a co-conspirator for assistance.

There are no exceptions to the warrant requirement that would deter an officer from obtaining a warrant to extract information from a cell phone when the phone is being taken to a

[159] Biddle, *supra* note 145.
[160] *Chimel*, 395 U.S. at 762-63.
[161] *Id*.

lab. Due to the time lapse between the arrest itself and the later extraction, a law enforcement officer has no excuse not to call a magistrate and obtain a warrant in order to avoid any potential Fourth Amendment violation.

2. IF THE EXTRACTION TECHNOLOGY IS BEING USED AT THE SITE OF ARREST

Companies such as Cellebrite maintain that their devices may be used in the field as well as a research lab.[162] Therefore, if law enforcement officers have mobile forensic technology equipment with them at the scene of an arrest, and have the required training necessary to effectuate a valid extraction, a warrant may not be required in such an instance to search the phone and further, seize the content of it.

Most courts which hold that searches of a cell phone without a warrant are reasonable follow the search incident to an arrest exception to the warrant requirement. The *Finley* court found the search substantially contemporaneous with the defendant's arrest.[163] Similarly, the *Diaz* court found that the "immediate association" of the cell phone with the defendant after his arrest entitled the police to inspect the phone's contents without a warrant.[164] If there is sufficient evidence that trained officers have conducted an on-site extraction of a valid arrestee's phone as a search incident to arrest, then no warrant would be necessary. Determining if the on-site extraction is sufficient without a warrant is a fact-based inquiry that must consider all of the possible warrant exceptions to the Fourth Amendment. At the scene of an arrest, it is likely that a warrant may not be necessary due to exigent circumstances such as safeguarding the police or the public from an ongoing crime, or protecting against the loss of evidence on the cell phone.

[162] Bennett, *supra* note 44.
[163] *Finley*, 477 F.3d at 253.
[164] *Diaz*, 244 P.3d at 505.

Another consideration for an on-site extraction is whether the cell phone is a container. Some courts have held that a cell phone does qualify as a closed container,[165] while other courts have held that a cell phone cannot be considered a container because it is not "capable of holding other physical objects."[166] Therefore, only if a cell phone is found to be a container pursuant to a valid inventory search, will a warrant not be required to search and extract information from the phone. If, on the other hand, a cell phone is not a container, then a warrant must be required to search and extract anything from it. The future of Fourth Amendment protections for cell phones depends on their being designated as "electronic containers," and thus, not searchable without a warrant.

3. Is there Such Thing as an Electronic Container?

The question of whether a cell phone can be characterized as a container, and thus searchable, has yet to be unanimously determined. The Supreme Court defined "container" in 1981, prior to the widespread use of cell phones, and did not specifically address "the authority to search a device's electronic memory."[167] Perhaps a new type of container—an "electronic container"—should be defined by all courts in the future to help resolve this issue.

A cell phone is able to store an enormous amount of digital information "inside" itself. With constant advances in cell phone technology, it may be time for the law to limit its definition of a container to exclude the digital content on cell phones, classifying "*electronic* containers" as an exception to the ordinary container exception. If courts adopt this definition of electronic containers, then law enforcement would be required to obtain a warrant before searching and extracting the data contained on the phones. Although cell phones are, by definition, containers,

---

[165] *See Finley*, 477 F.3d at 260.
[166] *See Smith*, 920 N.E.2d at 953.
[167] *Deans*, 549 F. Supp. 2d at 1094; *see also Belton*, 453 U.S. at 460-61 (defining a container as an object capable of holding another object).

albeit of digital content, the unique nature of this content justifies a new rule which excludes searching electronic containers as a valid inventory search incident to arrest. Due to the incredible amount of personal information that can be stored on a phone, such as medical and financial records, users have "a reasonable and justifiable expectation of a higher level of privacy in the information they contain."[168]

A cell phone qualifies as a container. While a digital piece of information is "wholly unlike any physical object found within a closed container," the information found within the cell phone is most likely the equivalent to the printed physical copy of the digital information.[169] Before cell phones were invented, the information now kept on phones would have necessarily been in physical form and carried in containers.[170] The capabilities of cell phones today, with respect to the amount and type of digital content stored on the phones, serve as a substitute for most of what people used to carry around as tangible objects and effects.[171] No longer is it necessary to carry address books, calendars, photo albums, or file folders; all of these can be contained in one small cell phone.[172] When "viewed in this light, the cell phone merely acts as a case (i.e. closed container)" holding one's personal effects.[173] Thus, since everything stored on a cell phone would be searchable if it were in its physical form, it seems logical that a cell phone should always be characterized as a container for purposes of a search.

Nevertheless, a cell phone contains electronic information that is *categorically* different from the physical information found inside ordinary containers. Although some cell phone content would have been found in a searchable physical form in the past, much of the

---

[168] *Smith*, 920 N.E.2d at 955.
[169] *Fawdry*, 70 So. 3d at 630 (citing *Robinson*, 414 U.S. at 235).
[170] *Fawdry*, 70 So. 3d at 630.
[171] *Id.*
[172] *Id.*
[173] *Id.*

information stored on phones today would not have been. For example, with advancements in electronic medical records, it is possible for someone to carry on their cell phone their entire medical history which, in tangible form, could fill boxes. Similarly, cell phones can store vast amounts of financial records that could presumably fill a filing cabinet. Cell phones can hold entire libraries full of books, or record stores full of music. The argument that a cell phone "merely acts as a case" or is a substitute for physically carrying one's effects is preposterous.[174]

While some courts have considered the term "electronic container" in the context of cell phone searches, they have explained that they fit within the ordinary container exception.[175] But modern cell phone capabilities justify that electronic containers be *excluded* from the ordinary definition, rather than become a subset of the container exception. If this were the case, warrants would be required, and citizens' reasonable expectation of privacy in their cell phones would be acknowledged and afforded constitutional protections.

D. PRIVACY ADVOCATES VS. LAW ENFORCEMENT

The technology created in order to extract information from cell phones is at the heart of contention between privacy advocates and law enforcement agencies. This year in Michigan, the American Civil Liberties Union received information that Michigan State Police were using Cellebrite UFED to extract information from cell phones during routine traffic stops.[176] In an interview, Mark P. Fancher, an ACLU Attorney for the Racial Justice Project, stated that "there

[174] See *infra* Part V, for a discussion of the immense amount of data available on a cell phone through cloud computing.
[175] *See* United States v. Cole, No. 1:09-CR-0412, 2010 U.S. Dist. LEXIS 82822, at *60-68 (N.D. Ga. 2010) (concluding that the defendant's cell phone was a "container" for purposes of applying an exception to the warrant requirement since it contained information not readily apparent without manipulating the cell phone itself); United States v. McCray, No. CR408-231, 2008 U.S. Dist. LEXIS 116044, at *13 (S.D. Ga. 2008) (concluding that "a cell phone, like a beeper, is an electronic 'container,' in that it stores information that may have great evidentiary value").
[176] Madrigal, *supra* note 2.

is great potential for abuse here, in that a police officer or a State trooper who may not be monitored or supervised on the street."[177]

The ACLU wrote a letter to the State Police requesting information regarding what mobile forensic devices were being used, how many were being used, how often, and why.[178] The letter also reiterated that using cell phone extraction devices, without the knowledge of the cell phone user, violates the Fourth Amendment.[179] The Michigan State Police, however, responded to the ACLU's request for information on their use of extraction devices by stating that "the State Police will provide information in accordance with the Freedom of Information Act…there may be a processing fee to search for, retrieve, review, examine, and separate exempt material" which has been estimated as costing those who request such information from the police at about $500,000. Fancher replies, "This should be something that they should be handing over freely. They should be more than happy to share with the public the routines and the guidelines that they follow."[180]

Michigan's response to the ACLU's letter should have a disturbing effect on every citizen and privacy advocate around the nation. If one state is allowing its law enforcement to use extraction devices without a warrant, it is likely that more states will follow in its lead unless laws are passed controlling this action. Otherwise, in a sense, our phones are becoming "our outboard brains," putting us in a "very difficult privacy position."[181]

Similarly, ever since the California Supreme Court's decision in *Diaz*, California civil rights advocates are coming forth in protest. For example, the Electronic Frontier Foundation

---

[177] *ACLU Says State Police Could Be Breaking 4th Amendment Rights*, CLICK ON DETROIT, http://www.clickondetroit.com/video/27563909/index.html (last visited Nov. 1, 2011).
[178] *Id*.
[179] *Id*.
[180] *Id*.
[181] Madrigal, *supra* note 2.

(EFF), a non-profit digital rights advocacy group, supports a California bill which would require state police officers to secure a warrant before searching an arrestee's cell phone.[182] In Oregon, the EFF filed an amicus brief on behalf of a criminal suspect who, forty minutes after being arrested and placed in a holding cell, had his cell phone "fished through" by an investigator, without a warrant, in order to uncover evidence related to his alleged crime.[183] Oregon officials maintained that the warrantless search was excused as being a search incident to arrest.[184] However, EFF senior staff attorney Marcia Hofmann maintained that "this is an empty excuse from the police—the suspect was in custody and unable to destroy evidence on his cell phone."[185]

Privacy advocates encourage cell phone users to set up passwords on their phones so that the phone's information and functions are less accessible to law enforcement. Catherine Crump of the ACLU stated that "the police can ask you to unlock the phone—which many people will do—but they almost certainly cannot compel you to unlock your phone without the involvement of a judge."[186] According to a 2009 study, 60% of people protect their phone with a password.[187] But, there are published guides available online that provide instructions on how to bypass passwords placed on cell phones.[188] Furthermore, mobile forensic technology can bypass passwords as well. While password-protecting one's phone makes it considerably harder for officers to search the phone, it does not make it impossible. Therefore, while password

---

[182] Amy Gahran, *Warrantless Cell Phone Searches Spread to More States*, CNN TECH (May 31, 2011), http://articles.cnn.com/2011-05-31/tech/warrantless.phone.searches_1_cell-phone-police-search-warrant-requirement?_s=PM:TECH.
[183] *Id*.
[184] *Id*.
[185] *Id*.
[186] *Id*.
[187] Richard P. Mislan, *Cellphone Crime Solvers*, IEEE SPECTRUM (July 2010), http://spectrum.ieee.org/computing/software/cellphone-crime-solvers.
[188] Declan McCullagh, *Police Push for Warrantless Searches of Cell Phones*, CNET (Feb. 18, 2010), http://news.cnet.com/8301-13578_3-10455611-38.html.

protecting cell phones is merely one step in securing privacy rights, these passwords do not guarantee privacy.

V. THE SCOPE OF SEARCHES, EXTRACTIONS, AND CLOUD COMPUTING: WHERE SHOULD COURTS DRAW A LINE?

A. CELL PHONES AND COMPUTERS

Often, searches of cell phones have been likened to searches of computers. Like warrantless cell phone searches, courts have come to varying conclusions on the constitutionality of a warrantless computer search. In *United States v. Forrester*, the Ninth Circuit held that police surveillance of a defendant's computer through a pen register analogue located at the Internet provider's facility was reasonable.[189] The two defendants in this case were arrested for various drug offenses and during the investigation, police officers set up surveillance of one of the defendants' computer to obtain e-mail addresses of outgoing e-mails, addresses of websites visited, and the total volume of information transmitted to and from his account.[190] The court concluded that the surveillance of the computer was analogous to the use of the pen register in *Smith v. Maryland* which the Supreme Court held to be constitutional and not a search under the Fourth Amendment since the information the pen register intercepted was being sent to a third party, the telephone company.[191] In its analysis, this court held that e-mail and Internet users, like the telephone users in *Smith*, relied on third-party equipment in order to communicate, thus their expectation of privacy in their e-mail or IP addresses of the websites they visited diminished.[192] Additionally, the court justified the computer surveillance on the grounds that the information obtained did not reveal the underlying content of the communication, but merely the

[189] United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2008).
[190] *Id.*
[191] *Id. See Smith*, 442 U.S. at 745.
[192] *Forrester*, 512 F.3d at 510.

e-mail addresses and IP addresses, just like the pen register in *Smith* only revealed telephone numbers.[193] The officers neither obtained the specific information from the body of the emails, nor the particular websites to which the IP addresses led.[194]

In *United States v. Arnold*, the Ninth Circuit concluded that a warrantless search of a defendant's laptop computer, separate hard drive, computer memory stick, and six compact discs was lawful based upon the "border-search doctrine."[195] While the defendant was waiting in line for customs upon returning to the United States from the Philippines, a U.S. Customs and Border Patrol Officer selected him for secondary questioning whereupon his luggage was searched and the laptop and its accessories were found.[196] After searching the computer and equipment, officers came across numerous images depicting child pornography which led to various charges against the defendant.[197] The district court held that, due to the nature of the private, personal and valuable information stored on one's computer, the search was invalid without a warrant or reasonable suspicion.[198] The Ninth Circuit, however, reversed and held that the warrantless search of the defendant's computer and equipment was valid under the border-search doctrine, and thus, no reasonable suspicion was required.[199] Under the border-search doctrine, searches of closed containers and their contents can occur at United States' borders "without particularized suspicion under the Fourth Amendment."[200] The justification for a border search is that the United States has the authority "to search the baggage of arriving international travelers" based

---

[193] *Id.*
[194] *Id.*
[195] United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008).
[196] *Id.* at 943.
[197] *Id.*
[198] *Id. See* United States v. Arnold, 454 F. Supp. 2d 999, 1007 (C.D. Cal. 2006).
[199] *Arnold*, 523 F.3d at 946. *Accord* People v. Endacott, 164 Cal. App. 4th 1346, 1347 (Cal. App. 2d Dist. 2008) (A search and seizure of the defendant's laptop computer and files was justified as a border search).
[200] *Id.* at 945. *But see* United States v. Montoya de Hernandez, 473 U.S. 531, 540-41 (1985) (restricting border searches to require reasonable suspicion to search one's "alimentary canal" because "'the interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusion [beyond the body's surface] on the mere chance that desired evidence might be obtained'") (citing Schmerber v. California, 384 U.S. 757, 769 (1966)).

upon "its inherent sovereign authority to protect its territorial integrity."[201] Thus, "by reason of that authority, [the United States] is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry."[202]

By contrast, in *United States v. James*, the Eighth Circuit suppressed information discovered on computer discs given to police by a third party.[203] The defendant in this case was arrested for sexual misconduct involving a child and, while in jail, wrote a letter to a third party instructing him to destroy certain computer discs.[204] Detectives intercepted the letter and went to the third party's home, without a warrant, where they obtained the discs and then viewed the content of the discs at the police station.[205] The discs contained images of child pornography.[206] The court ultimately held that the detectives' actions violated the Fourth Amendment's warrant requirement because not only did the third party lack authority to consent to the search, as he had no established common authority in owning the discs, but also no valid exception to the warrant requirement applied to justify the detectives' behavior.[207]

In the Washington court of appeals, a defendant was arrested on suspicion of auto theft.[208] While searching the defendant's car, a laptop computer was found inside of a bag.[209] Suspecting that the laptop was stolen, the officer brought the computer to the police station where another officer searched the computer files for information about its lawful owner.[210] Based upon the information found in the computer, the officers were able to contact the

---

[201] Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979).
[202] *Id*.
[203] United States v. James, 353 F.3d 606, 610 (8th Cir. 2003).
[204] *Id*. at 611.
[205] *Id*.
[206] *Id*.
[207] *Id*. at 617.
[208] State v. Washington, No. 47773-1-I, 2002 Wash. App. LEXIS 142, at *1 (Wash. Ct. App. Jan. 28, 2002).
[209] *Id*. at *2.
[210] *Id*.

computer's rightful owner and establish that the computer was stolen by the defendant.[211] Although the court found that the police had probable cause to both arrest the defendant and seize the computer from the bag in the car, it concluded that the subsequent search of the computer's files was unlawful without a warrant.[212] The court explained that "probable cause to believe property is stolen does not itself justify an investigative search of that property."[213] Instead, "compliance with the warrant requirement is necessary to ensure that the police are justified in invading a person's privacy interest to search for evidence."[214]

As the varying case law demonstrates, it might seem obvious that with the cell phone technology available today, "the line between cell phones and computers has become increasingly blurry."[215] As there is still no unanimous precedent guiding all courts to address cell phone or computer searches the same way, our Fourth Amendment privacy rights remain in question. Consequently, our rights regarding cloud computing—a quickly growing phenomenon that impacts both cell phones and computers—will likely be affected by this uncertainty.

B. CLOUD COMPUTING AND GROWING PRIVACY CONCERNS

Cloud computing is the act of storing and accessing applications and computer data through the Internet, or a web browser, rather than running installed software on one's personal computer, such as Microsoft Word or Excel.[216] In essence, "every piece of data you need for every aspect of your life" is made available "at your fingertips and ready for use" by cloud computing.[217] It allows you to "sync up your devices" and access all of your content on

---

[211] *Id*.
[212] *Id*. at *4, *8.
[213] *Id*. at *8.
[214] *Id*.
[215] *Park*, 2007 U.S. Dist. LEXIS 40596, at *23.
[216] CLOUD COMPUTING, http://www.cloudcomputingdefined.com/ (last visited Nov. 29, 2011).
[217] Rivka Tadjer, *What is Cloud Computing?* PC MAG (Nov. 18, 2010), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

"whatever device [you] have, wherever [you] happen to be."[218] Cloud computing also gives users the ability to share all data, photos, contacts, documents, music, and more with others in an instant, as well as gain access to the "public cloud and other personal clouds."[219]

Any device with Internet access can take advantage of the cloud. Smartphones can easily synchronize with e-mail, social media, word-processing, or music programs that can then be accessed from any location and shared with whomever the user chooses. Additionally, smartphones can synchronize with computers to give users the option to access their computer through their phone. But what does this mean for our privacy rights? We do not know and neither does the current law.

Synchronizing computers with cell phones exposes the cell phone user to myriad privacy issues. One of the major aspects of cloud computing is that third-party service providers store information in the cloud for one's personal access. The rule from *Smith v. Maryland*, that a person has no reasonable expectation of privacy in information turned over to third parties, seems to be applicable in the consideration of cloud computing.[220] When one creates a personal cloud, accessing the cloud from a smartphone must come through a third party, whether it is Google, Facebook, Twitter, Outlook, and so forth. Therefore, since everything on a computer can be placed on the cloud, and further accessed through a smartphone, then under *Smith*, there is no reasonable expectation of privacy in any of this information. Consequently, law enforcement can search and extract all of this information without a warrant. What a scary thought. Although applying the *Smith* rule in this context is logical, citizens still anticipate having an expectation of privacy in their smartphones, even if they are accessing a cloud. It is unreasonable to accept that

[218] *Id.*
[219] *Id.*
[220] The *Smith* third party rule has been cited consistently since its first application. *See, e.g.*, United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011) (citing *Smith*).

simply using the cloud would permit the government to search and extract all of the content from our phones. In an effort to protect citizens' constitutional rights, while still maintaining a strong criminal justice system, the scope of what the government can search and extract from cell phones must be limited.

C. WHERE SHOULD COURTS DRAW THE LINE?

As the law stands today, the government has numerous ways of accessing the content stored on one's cell phone and computer, either through a warrantless search permitted under the Fourth Amendment or by accessing the cloud. The scope of this access, however, must be controlled. A line must be drawn somewhere, but as the law continuously struggles to keep up with emerging cell phone technology, it is unclear where this line will be.

Recently in *United States v. Maynard*, the Court of Appeals for the District of Columbia Circuit considered, among other claims, the scope of a warrantless search that took place by placing a GPS monitoring device on a co-defendant's car in order to further a drug investigation.[221] In this case, the police installed the GPS device on the co-defendant's car without a warrant and monitored his movements twenty-four hours a day for four weeks.[222] While this case concerned a warrantless search of a GPS device rather than a cell phone, the co-defendant's reasonable expectation of privacy was still at issue. The court expressed concern with the expanding application of the Fourth Amendment exceptions, and it determined that the monitoring of the car constituted a search and violated the co-defendant's reasonable expectation of privacy.[223] A novel question emerged: to what extent does "comprehensive" and "sustained"

[221] United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010), *cert. granted*, United States v. Jones, 131 S. Ct. 3064 (June 27, 2011).
[222] *Maynard*, 615 F.3d at 555.
[223] *Id*.

surveillance trigger Fourth Amendment protections?[224] The police were able to discover "the totality and pattern of [the co-defendant's] movements from place to place," not merely "movements from one place to another."[225] While the government maintained that the search was valid because the co-defendant's actions were exposed to the public, so he could have been followed everywhere he went on public roads, the court held that "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[226] The court further held that the information discovered by the police using the GPS was not "constructively exposed to the public."[227] The court likened the GPS surveillance to a rap sheet and explained that the prolonged surveillance "reveal[ed] types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble."[228] In conclusion, the court held that the GPS monitoring "defeat[ed] an expectation of privacy that our society recognizes as reasonable."[229]

In many ways, the GPS surveillance in *Maynard* can be analogized to searches of cell phones and access to personal clouds. Like the twenty-four hour tracking of the co-defendant, searching and extracting content from one's cell phone gives police officers a detailed picture of the cell phone user's life. An issue the D.C. Circuit faced was that the surveillance was sustained for a long period of time. It was neither a one day occurrence nor a specific search that ended quickly. Obtaining *some* data, text messages, contacts, or pictures from a cell phone is equivalent to a short surveillance that could potentially be valid if the search is limited in scope

[224] *Id*. at 556.
[225] *Id*. at 558.
[226] *Id*. at 560.
[227] *Id*. at 561.
[228] *Id*. at 562.
[229] *Id*. at 564.

and has a reasonable end point. But if law enforcement is able to get *all* information from a cell phone or through a cloud, therefore reaching a computer, this search is the equivalent of the unconstitutional twenty-four hour a day, four week surveillance in *Maynard*. Such a comprehensive search would uncover vast amounts of private information. It is exactly this type of information gathering that the *Maynard* court held unconstitutional as a violation of society's reasonable expectation of privacy in such content. Further, like the GPS information, the information contained on a cell phone is not "constructively exposed to the public," even if it can be shared via cloud computing. The content shared on a cloud can be selectively chosen, and if one so chooses, the cloud can remain "personal" and therefore, private.

Just as privacy advocates are paving the way for courts to address extraction technology, The Digital Fourth Amendment Campaign has been created to lobby the government to create search and seizure laws that are up-to-date with today's digital world. The coalition "is dedicated to bringing obsolete laws…into the digital age."[230] Specifically, the campaign is asking Congress to "amend outdated U.S. laws originally intended to protect citizens against unwarranted governmental access to their private information held electronically by third parties."[231] The campaign maintains that "the laws protecting such information have been eroded by technological change."[232] It recognizes the current gaps in legal protection that American citizens face and asserts that "Congress can restore Americans' individual liberties in the digital age and ensure the Internet remains a powerful engine of economic growth, while

---

[230] Warner Todd Huston, *Does Government Own Your Remotely Backed Up Computer Files, Your Emails, or Your Cell Phone GPS Info?*, PUBLIUS' FORUM (Apr. 6, 2011, 10:25 AM), http://www.chicagonow.com/publius-forum/2011/04/does-government-own-your-remotely-backed-up-computer-files-your-emails-or-your-cell-phone-gps-info/.
[231] *ECPA Letter: Digital Fourth Amendment Coalition Letter*, DIGITAL FOURTH AMENDMENT, http://www.digitalfourthamendment.org/ecpa-letter/ (last visited Nov. 29, 2011).
[232] *Id.*

preserving the tools needed by law enforcement investigations and removing legal uncertainty that may hamper law enforcement's effectiveness."[233]

VI. CONCLUSION

The Fourth Amendment's application, and criminal procedure in general, is being challenged by the growth of a technologically sophisticated, cell phone-using society. As cell phones advance, the law too must advance. It is no surprise that this is a difficult task facing all courts today since, "given their unique nature as multifunctional tools, cell phones defy easy categorization."[234]

Law enforcement agencies recognize that they are struggling to keep up with quickly changing mobile technology. In response, "this is forcing them to make new and perhaps strange ethical choices."[235] The ability of law enforcement to search cell phones will no doubt be an advantage for the government in prosecuting cases, but courts will encounter challenging Fourth Amendment questions relating to these searches, especially when they result in extraction through mobile forensic technology. As courts are faced with evidence from extraction devices, case law will emerge, and complicated Fourth Amendment analyses will be undertaken regarding the admissibility of the extracted data.

Until clear precedent is established, warrantless cell phone searches and extractions will continue to be an issue. But, if courts choose to limit container searches to exclude cell phones, designating them as "electronic containers," law enforcement would always be required to obtain warrants before searching and extracting the data contained on phones. If warrants become required to search and extract electronic containers, mobile forensic devices will relieve any fear

[233] *Id*.
[234] *Smith*, 920 N.E.2d at 955.
[235] Madrigal, *supra* note 2.

that the information on the phones will be lost or overridden due to the time delay in securing a warrant, since these devices are able to retrieve any deleted information from the phones.

Cell phones today are capable of telling its user's entire life story. With cloud computing, and the option of synchronizing computers with cell phones, one becomes exposed to countless privacy issues. In particular, whether *Smith*'s third party rule will continue to apply in such a situation, thereby making everything on one's personal cloud void of a reasonable expectation of privacy and thus, searchable. Due to the incredible amount of personal information capable of being found on cell phones, it is reasonable for citizens to expect a high level of privacy in this information. As evidenced by groups such as the ACLU, EFF, and The Digital Fourth Amendment Campaign, our Fourth Amendment rights are in jeopardy. It is not only daunting, but unacceptable, if our laws are not updated accordingly so as to fairly address the concerns of citizens, law enforcement, and privacy advocates alike.

In today's society, cell phones and other forms of technology are the most highly recognized forms of communication. These devices are ubiquitous in everyday life. We depend on cell phones to keep our lives in order, to communicate, to assist, and to memorialize. It is only fitting that citizens' expectations of privacy in their cell phones be recognized and afforded the full weight of Fourth Amendment protections.