1-1-2010

Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence

Matthew E. Orso

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
CELLULAR PHONES, WARRANTLESS SEARCHES, AND THE NEW FRONTIER OF FOURTH AMENDMENT JURISPRUDENCE

MATTHEW E. ORSO*

INTRODUCTION

Advances in technology and science have always presented challenges in applying constitutional search and seizure law. In this context, the Supreme Court has considered whether law enforcement may, absent a warrant, eavesdrop on private telephone conversations and use radio transmitters to track the public and private movements of suspects. The Court has addressed whether the aerial surveillance of land and the use of a thermal imaging device to gather information about the inside of a home constitute searches under the Fourth Amendment. Further, it has tackled such issues as the legality of mandatory urinalysis for

*J.D., Saint Louis University School of Law, 2009. I am grateful to Professor Eric J. Miller for his insightful comments and guidance. Thanks also to Professor Adam Gershowitz for helpful comments and suggestions during the revision process, and to Professor Orin Kerr for pointing me in the direction of some of his recent analysis on the topic. Finally, special thanks are due to Chief Judge Catherine D. Perry of the U.S. District Court for the Eastern District of Missouri, who sparked my interest in this topic long ago with a research project and thought-provoking conversation. All opinions expressed are the author's own.

high school athletes and chemical field-testing of suspected drugs that have been seized by law enforcement.

Yet as one court has appropriately observed, "[t]he recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored." A quick glance at the edge of this new frontier might reveal the following: the FBI’s "Magic Lantern" technology, a Trojan horse virus that remotely injects surveillance programs onto a suspect's computer and records every keystroke; X-ray devices that allow law enforcement to see through people's clothing; and police tracking of the geographical location of a cellular phone (and its owner) by obtaining the service provider's records without probable cause or a warrant. There are countless examples, but all hold at least one trait in common: Fourth Amendment questions abound while legal precedent often lacks, leading to tenuous conclusions.

This article explores a tiny thread of this vast new frontier. In particular, it explores one intersection between technology and Fourth Amendment jurisprudence that has ballooned in commonality, yet remains untouched by the Supreme Court—the warrantless search of a cellular phone's contents.

Law enforcement officers often search the contents of a suspect's cellular phone without obtaining a warrant. In response, defendants have challenged these searches in recent years. The Government has defended the legality of

7. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008).
10. See, e.g., In re Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).
11. See, e.g., United States v. Finley, 477 F.3d 250, 255 (5th Cir. 2007); United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *5 (N.D.
warrantless cellular phone searches by way of various exceptions to the warrant requirement, including, most commonly, the search incident to arrest and exigent circumstances exceptions. Further, federal courts have regularly upheld these searches, rarely invalidating them for want of a warrant.

Many issues arise in considering the legality of a warrantless search of an individual’s cellular phone. Part I of this article establishes a point of reference for analyzing the issue by distinguishing between different types of information. It distinguishes between information stored on a cellular phone as opposed to data stored on a third-party server, and it further differentiates between the various types of information stored on a cellular phone. Part II analyzes the implications arising from the search of a cellular phone’s “coding information.” Part III considers the issues raised by the search of a cellular phone’s “content-based” information. Part IV examines recent judicial decisions applying various warrant requirement exceptions to the search of a cellular phone’s contents. It then proposes a new standard for searching cellular phones incident to arrest. Finally, Part V examines the move toward instruments, such as the iPhone and G2, which appear more akin to personal computers than telephones in terms of their functionality and capacity for information storage. These newer devices create difficult new Fourth Amendment problems for which there has been little analysis in either the courts or academia. Part V further proposes a different standard for searching these devices than the standard proposed for older generation cellular phones in Part IV of this article.

I. DISTINGUISHING BETWEEN TYPES OF INFORMATION

Telephonic communication has long presented constitutional privacy concerns. Originally, those concerns revolved around various forms of electronic eavesdropping by law enforcement. Later, they expanded to include information, such as telephone numbers, transmitted to

Cal. May 23, 2007).
12. See infra Parts IV.A–B.
13. See infra Parts IV.A–B.
phone companies as part of the process of connecting a call. More recently, these privacy concerns have further expanded with the advent of cellular phones and newer, more advanced "smart phones." These cellular devices have changed the landscape dramatically.

This article considers the private information—including call lists, text messages, address books, and photographs—actually stored on a cellular phone. Information stored on third-party data servers presents different, yet equally challenging, legal issues. While data on a third-party server is often identical to information stored on a cellular phone (i.e., the same call list or text message that is stored on the phone), a government search of this information raises unique questions, such as whether the service provider was a "party" to the communication and whether a subpoena, rather than a warrant, is a legal means of obtaining the information.

Data stored on an individual's cellular phone, on the other hand, concerns a private container. When the government seeks to access this information, the Fourth Amendment governs the legality of such action. Searching a cellular phone's contents not only raises search issues, but also questions as to whether the phone's seizure was legal. Further, this data is clearly held by a party to the communications, unlike the uncertainty regarding a third party who owns a data server. While the character of the information is the same in both scenarios, the different location and possessor of the information give rise to different questions, and potentially deviating outcomes. This article considers the information stored on a cellular phone, leaving server data for another occasion.

One important consideration regarding information's

---

17. This article does not consider the issue of the legality of a cellular phone's seizure, as the analysis of such a seizure does not seem to differ much from the analysis that pertains to other types of containers and personal items. Cf. State v. Washington, No. 47773-1-I, 2002 WL 104492 (Wash. Ct. App. Jan. 28, 2002) (holding seizure of a laptop incident to suspect's arrest legal, while search of the laptop was illegal).
18. See supra note 16 and accompanying text.
Fourth Amendment protection is whether it is information in which the owner has a reasonable expectation of privacy. If a person holds a subjective expectation of privacy in the information, and if this expectation is one society recognizes as reasonable, then law enforcement's viewing or obtaining that information from the phone constitutes a search under the Fourth Amendment. If, however, there is no reasonable expectation of privacy in the information, then there is no Fourth Amendment search. Therefore, when considering the legality of a search of a cellular phone's contents, it makes sense to consider (1) whether a phone's owner has a reasonable expectation of privacy in the general contents of a cellular phone, and (2) whether some information is the subject of a reasonable expectation of privacy while other information is not.

Another important distinction must be addressed. Not all information stored on a cellular phone is of the same ilk, because some stored items are far more private than others. Consider a very personal text message, or a private photograph captured with a camera phone. These items are naturally more private than less personal information, such as a list of recently dialed telephone numbers or an address book. The varying degrees of privacy expectations that attach to these different types of information may lead to different Fourth Amendment conclusions about the legality of a search.

Accordingly, this article distinguishes between two different types of data that law enforcement seeks to obtain: "coding information" and "content-based information." Coding information describes information that merely identifies the parties to a communication. This information includes phone numbers, email addresses, pager numbers, and any label that uniquely identifies an account. This information is similar to the return or receiving address printed on an envelope, which uniquely identifies a location.

19. See Katz, 389 U.S. at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").
20. See id.
21. See id.
22. See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (analogizing the number dialed in sending a text message to the address printed on the envelope of a letter).
It tells a third party where to deliver the letter, but it does not reveal the handwriting inside. Content-based information describes (1) the substance of a communication and (2) a privately stored piece of information reserved for personal use. This information includes text messages, emails, voicemails, digital photographs, and other data.

The characterization of information as either coding or content-based may bear on its level of Fourth Amendment protection. If a type of information is not the subject of a reasonable expectation of privacy, then the Fourth Amendment does not protect it, because viewing it is not considered a search. Further, even if coding and content-based information are both subjects of a reasonable expectation of privacy, this distinction may aid in developing an appropriate standard by which searches incident to arrest may be conducted. The next two sections of this article consider this distinction, analyzing separately the implications for both coding and content-based information.

II. CODING INFORMATION

Coding information describes data that reveals only the identity of a party to a communication without disclosing the subject matter of that communication. It consists of phone numbers, email addresses, pager numbers, and other labeling information that uniquely identifies an account. In the context of cellular phones, coding information consists of phone numbers that are usually contained in a list of recently dialed or recently received calls or text messages. This information tells its observer the identity of the other party to a call or text message, but it does not reveal the content of that call or message.

If a person has a reasonable expectation of privacy in the coding information contained in her cellular phone, then an officer’s examination of that data constitutes a search under the Fourth Amendment. If, however, there is no reasonable expectation of privacy in the coding information stored on the phone, then examining that information does not constitute a search, and a warrant (or warrant exception) is not required. One then must determine whether an individual holds a reasonable expectation of privacy in the coding information.

Coding information is the same kind of information that law enforcement regularly obtains without a warrant by using pen registers and trap-and-trace devices. A pen register is a device that records the phone numbers associated with outgoing calls from a particular phone. A trap-and-trace device records the phone numbers of incoming calls. The Supreme Court has long held that police may use these devices to record phone numbers. The Court has reasoned that when a person shares this information with his telephone company by sending or receiving a call, he does not have a reasonable expectation of privacy in the phone number at the other end of the call or text message.

Although this article focuses upon the information that is stored on a cellular phone rather than information that is intercepted en route to its destination, the character of the information is the same—a particular telephone number.

24. This article assumes in its discussion that the person in possession of a cellular phone is its owner, and not a borrower or some other non-owner. While at least one circuit court has stated that "mere possession of a cell phone gives rise to a reasonable expectation of privacy regarding its contents," United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008), different questions arise from a non-owner scenario. These questions are not considered here for reasons of length and author interest.


27. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).


29. Id. ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required."). Congress authorized the use of pen registers and trap-and-trace devices in the Electronic Communications Privacy Act of 1986. 18 U.S.C. § 3121 (2006). It later expanded the scope of information these devices can legally capture to include information pertaining to Internet communications, such as email addresses, in Section 216 of the USA Patriot Act of 2001. 18 U.S.C. §§ 3121–3125 (2006). The Act importantly limits the use of pen registers and trap-and-trace devices to capturing "dailing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." § 3121(c) (emphasis added).
Therefore, one must ask why, if law enforcement can obtain the information from a pen register or trap-and-trace device without a warrant, the same should not hold for the identical information stored on a cellular phone. The data exists in a different location (stored on a phone versus en route to a destination), but is the reasonable expectation of privacy in the information on the phone not already lost when a call is sent or received? After all, this information was shared with the cellular service provider and exposed for interception by pen registers and trap-and-trace devices.

Here, location is the key. When data has not been intercepted, but *could have been* via a pen register, it is very different than if the data actually *had been* intercepted. Justice Scalia makes a similar argument in *Kyllo v. United States*, where law enforcement used a thermal imaging device to gather heat images of a suspect's home. In holding that a Fourth Amendment search had occurred, Justice Scalia explains: "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."

A basic analogy may shed further light on this point. Imagine that you send a letter to a friend. Nothing stops law enforcement from observing the information on the outside of the envelope while the letter is in the custody of the postal service. However, if law enforcement does not obtain that information while the letter is in transit, the opportunity is lost. Once the letter reaches a person's mailbox, or at least the inside of his home, it has entered a location in which an owner has a reasonable expectation of privacy. Similarly, once the information sent from a cellular phone is no longer in transit, it is no longer obtainable by a pen register.

---

31. *Id.* at 35 n.2 ("The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful."). Understandably, *Kyllo* dealt with privacy in relation to the home, but the reasoning applies well to the difference between intercepting information via a pen register as opposed to illegally obtaining information from the memory of a cellular phone.
32. *See United States v. Karo*, 468 U.S. 705, 732 (1984) ("It is certainly true that a homeowner has a reasonable expectation of privacy in the contents of his home, including items owned by others.").
33. It is, however, potentially subject to a subpoena served upon the cellular service provider. *Cf. Smith v. Maryland*, 442 U.S. 735, 735–36 (relying on
Therefore, the incoming and outgoing phone numbers stored in recent call lists are like the letter that has already been delivered—they are now in a protected area.  A different outcome would create a Fourth Amendment black hole for any area where information exists after the fact, as long as law enforcement could have previously viewed it.

Most courts seem to agree, at least implicitly, with this analysis, as they have not often considered this distinction between coding and content-based information. Instead, they have analyzed phones' contents as a whole. In so doing, courts have regularly dismissed the suggestion that a person does not have a reasonable expectation of privacy in the general information (both coding and content-based) stored in his cellular phone. For example, the government argued in one case that searching a cellular phone's contents during an investigative stop was akin to running a license check during a traffic stop. In response to this argument, the Fifth Circuit stated that “[u]nlike a driver’s license and vehicle registration, which are typically issued by a governmental entity, cellular phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. [The defendant] had a reasonable expectation of privacy regarding this information.” In this same regard, courts have regularly held that a person has a reasonable expectation of privacy in the contents of his cellular phone. Thus, absent an applicable exception, law enforcement must obtain a warrant even if it only seeks to search a cellular phone for coding information.

United States v. Miller, 425 U.S. 435, 442 (1976) (holding bank records obtainable by subpoena because privacy expectation was lost when records were conveyed to bank employees)); supra note 16 and accompanying text.

34. The outgoing call list is more appropriately analogized to a written log of all addresses to whom one has sent letters. It is unique in that it is an internal record, and thus different from information that is sent via a third party.

35. But see infra note 132 and accompanying text (discussing courts that have noted such a distinction in substance, if not in name).

36. United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008).

37. Id. (citing United States v. Finley, 477 F.3d 250, 258–59 (5th Cir. 2007)).

38. See, e.g., Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008); Finley, 477 F.3d at 258–59. In addition, the Ninth Circuit recently held that government employees have a reasonable expectation of privacy in text messages they send, even when the messages are stored on the service provider's server. Quon, 529 F.3d at 910.
Professor Orin Kerr has observed:

[Courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies. For better or for worse, courts have tended to apply the same property-based principles to such cases that they have applied elsewhere. This has focused attention on whether government investigators collect information that technology has hidden or information that technology has exposed.]

This statement may shed light on the general agreement of the courts that a cellular phone's owner holds a reasonable expectation of privacy in its contents. A cellular phone is a piece of physical property that must be manipulated before the information stored within is exposed. In a way, technology has "hidden" the information stored inside it, such as photographs that would otherwise be printed on paper or text messages that otherwise might be written on paper. This property-based focus looks to protect cellular phone users, at least initially, in determining that viewing and seizing a cellular phone's contents is a search. This article later explains, however, that classifying it as a search under the Fourth Amendment has so far presented only a minor hurdle to prosecutors in attempting to use evidence of a cellular phone's contents at trial. Thus, a privacy-based view, rather than a rudimentary property-based view, is necessary to conform to Fourth Amendment standards in the cellular phone context, even if courts would rather not engage in such an inquiry.

As a matter of practicality, the coding/content-based distinction may seem of little significance at first glance. Regardless of one's characterization of the data, if the information is stored on a cellular phone, then its owner has a

---


40. In speaking of information that technology exposes, Professor Kerr points to technology that law enforcement uses to obtain information in ways that it previously could not. See id. at 828–30 (citing California v. Ciraolo, 476 U.S. 207 (1986) (discussing aerial surveillance of land using airplane); United States v. Jacobsen, 466 U.S. 109 (1984) (discussing chemical testing of substance for presence of illegal narcotics); Smith v. Maryland, 442 U.S. 735 (1979) (examining use of pen register to obtain telephone numbers)).
reasonable expectation of privacy in it. But if courts continue their regular practice of upholding warrantless searches of cellular phones, this distinction will help place a limit on what information the government can access. To this end, when police search a suspect's cellular phone incident to his arrest, the coding/content-based distinction provides a useful line of demarcation (or a helpful starting point at least) between what police may view and what they may not.

III. CONTENT-BASED INFORMATION

The Fourth Amendment should grant significant protection to content-based information because, unlike coding information, it consists of the subject matter of a communication as well as privately stored data reserved for one's personal use. As noted above, this category includes the actual text message rather than the mere address of the recipient or sender; it further includes private information stored on a phone, such as digital photographs, videos, and personal memos.

Pen registers and trap-and-trace devices do not record content-based information, and therefore no analogy regarding these devices needs consideration. But how protected is content-based information as compared to coding information? Should content-based information receive greater protection than coding information? This brief section examines judicial treatment of content-based information, finding in the limited case law a general view that an owner and possessor of content-based information has a reasonable expectation of privacy in it.

Courts have found that content-based information deserves more protection than coding information, without using these specific terms. For example, the Ninth Circuit held in Quon v. Arch Wireless Operating Co. that users of text messaging services have a reasonable expectation of privacy in their text messages stored on the service provider's network. The court quoted Smith v. Maryland, stating that "a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the

41. See infra Part IV.A–B.
42. Quon, 529 F.3d at 904.
43. Smith, 442 U.S. 735.
contents of communications." To the Ninth Circuit, the contents of text messages were naturally more like the live conversation in Katz than the telephone numbers in Smith.\textsuperscript{45} Thus, even when stored outside the user’s pager and on a third-party server, the contents of the messages were still protected by the communicating party’s reasonable expectation of privacy.\textsuperscript{46} It follows that when text messages are stored on an actual phone, there is little question that the phone’s owner has a reasonable expectation of privacy in the messages.\textsuperscript{47}

Email, now accessible via modern devices like the iPhone and G2 (“smart phones”), has received relatively little treatment in the courts in terms of its content-based nature.\textsuperscript{48} Email, unlike text messages, is most regularly stored on third-party servers. However, if a user sets up a Package on Package account, then the email messages can be downloaded onto the phone and stored there rather than on a remote

\begin{itemize}
\item \textsuperscript{44} Quon, 529 F.3d at 904 (quoting Smith, 442 U.S. at 741).
\item \textsuperscript{45} See id. at 904–05.
\item \textsuperscript{46} Id. at 905–06; see also United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (discussing whether the defendant had a reasonable expectation of privacy with regard to text messages stored on a phone); United States v. Finley, 477 F.3d 250, 258–59 (5th Cir. 2007) (considering whether the defendant had a property or possessory interest in a phone on which he sent text messages).
\item \textsuperscript{47} If nothing else, just like with coding information, the location alone of the text messages should dictate that a reasonable expectation of privacy attaches. See supra notes 35–37 and accompanying text.
\item \textsuperscript{48} Before being vacated en banc for ripeness, a Sixth Circuit panel determined that emails are protected as content-based. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (6th Cir. 2008). The Warshak court held that email users have a reasonable expectation of privacy in the contents of their emails stored with an Internet service provider (“ISP”). Id. Even though the user agreement with the ISP granted the company the reserved right to access a user’s emails, the court held that the emails were protected because ISP employees do not regularly read subscribers’ emails. Id. at 474. Consistent with this view, the Ninth Circuit has held that an email user does not have a reasonable expectation of privacy in the mere identifying information attached to an email (i.e., the subject heading and address). United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007). These holdings adhere to the coding/content-based distinction, at least regarding information stored with a third party and not on a cellular phone. No other circuit has addressed the issue, and few district courts have examined it either. But see United States v. Polizzi, 549 F. Supp. 2d 308, 393–94 (E.D.N.Y. 2008) (“Courts have generally found a reasonable expectation of privacy in the email messages themselves.”); United States v. Maxwell, 45 M.J. 406, 417–18 (C.A.A.F. 1996).
\end{itemize}
When emails are stored on the phone, the same analysis for text messages stored on a phone should apply to email because of the nearly identical function of the two media.

In addition, digital photographs are content-based information for which an owner of a phone has a reasonable expectation of privacy. This content is similar to all strains of coding and content-based information that are stored within cellular phones in that it exists in the actual phone, concealed from view. Photographs and videos, however, are potentially even more sensitive and private than other forms of content-based information, for obvious reasons. It is photographs and videos, among other content, that may justify an argument limiting the scope of searches of cellular phones incident to arrest. This issue is taken up in Part IV.D.

Thus, users have a reasonable expectation of privacy in content-based information stored on their cellular phones. The terrain does become less clear for content-based information stored on third-party servers. In fact, for text messages and emails stored on third-party servers, depending on ISP user agreements and other factors, the existence of a reasonable expectation of privacy is not without some doubt. But for purposes of this section, it is enough to state that the Fourth Amendment is implicated when officers search the content-based information stored in a cellular phone.

Stepping back from the coding/content-based distinction, one might view the issue as simply as the Supreme Court stated in United States v. Ross: "[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view." While this statement certainly pertains to the contents of a cellular phone,

---


50. Of course, information displayed on the face of the phone and easily observable by others, like a wallpaper photograph on the home screen of a phone, would not hold a subjective or objective expectation of privacy.

discussing the coding/content-based distinction allows the consideration of a number of interesting questions. Further, Part IV.D of this article revisits this distinction in attempting to determine whether and how to limit the scope of various cellular phone searches to protect citizens’ basic Fourth Amendment rights against unreasonable search and seizure. Before this attempt, however, more examination must be given to the developing jurisprudence regarding the warrantless search of cellular phones.

IV. JUDICIAL ANALYSES OF WARRANTLESS CELLULAR PHONE SEARCHES

This section examines various circuit and district court analyses of warrantless cellular phone searches. It highlights a budding legal fiction in the application of the exigent circumstances exception and an emerging ideological divide in the application of the search incident to arrest exception. Although to lawfully search a cellular phone’s contents, law enforcement must first lawfully seize the phone, this section will not address the seizure issue because the fact that the container is a phone adds little to the seizure analysis.

As discussed prior, when officers examine a cellular phone’s contents, a Fourth Amendment “search” occurs. The more difficult question arises, however, when officers fail to obtain a warrant before engaging in such a search. Do officers need a warrant to search the information stored on a cellular phone? One would assume so, since the search implicates Fourth Amendment protections. However, a review of case law suggests the opposite. More often than not, federal courts have validated warrantless searches of cellular phones, usually relying on one of two exceptions to the warrant requirement—exigent circumstances and search incident to arrest. Courts applying the exigent circumstances exception to allow warrantless searches of cellular phones may be furthering a new legal fiction—that an exigency exists merely because information is stored on a cellular phone. In addition, there is a growing divide among courts in their application of the search incident to arrest exception such that, faced with the same facts, a handful of

52. See supra Parts II, III.
53. See infra Parts IV.A, B.
courts would invalidate a warrantless search of a cellular phone incident to arrest while many more would uphold it.

A. The Exigent Circumstances Exception

The Supreme Court has held that "[w]here there are exigent circumstances in which police action literally must be 'now or never' to preserve the evidence of the crime, it is reasonable to permit action without prior judicial evaluation." This statement is the essence of the exigent circumstances exception to the warrant requirement. It has been applied to a broad scope of scenarios, including warrantless home and automobile searches. Courts have more recently applied this exception in the context of cellular phone searches.

A case from the District of Kansas provides a good example of the rationale federal courts have used in upholding warrantless cellular phone searches based on exigent circumstances. In United States v. Parada, officers properly seized a defendant's cellular phone during the course of an inventory search of a van. At the warehouse where the inventory search took place, an officer searched the contents of the cellular phone, looking at the phone numbers in the list of recent calls and recording them. The government argued that this search was justified, because had the phone received additional calls, numbers in the recent call list would have been lost. The court upheld the search under the exigent circumstances exception. It

55. Warden v. Hayden, 387 U.S. 294, 298 (1967). In Warden, the Supreme Court held that officers' hot pursuit of a suspected criminal into a residence created an exigency that alleviated the need for a warrant to enter and subsequently search a home. Id.
56. Chambers v. Maroney, 399 U.S. 42, 51 (1970). Exigent circumstances justify the original rationale behind the automobile exception to the warrant requirement because an automobile's inherent mobility creates the exigency that evidence will be lost or removed from the jurisdiction and out of a warrant's reach. See California v. Acevedo, 500 U.S. 565, 591 (1991) (citing United States v. Ross, 456 U.S. 798, 822 (1982)). Later cases have strayed from the notion that an exigency is required to trigger the automobile exception, citing the reduced privacy expectation regarding vehicles because of their "pervasive regulation." California v. Carney, 471 U.S. 386, 392 (1985) (citation omitted).
58. Id. at 1297.
59. Id. at 1303.
60. Id. at 1303–04.
reasoned:

Because a cell phone has a limited memory to store numbers, the agent recorded the numbers in the event that subsequent incoming calls effected the deletion or overwriting of the earlier stored numbers. This can occur whether the phone is turned on or off, so it is irrelevant whether the defendant or the officers turned on the phone.

Under these circumstances, the agent had the authority to immediately search or retrieve, as a matter of exigency, the cell phone's memory of stored numbers of incoming phone calls, in order to prevent the destruction of this evidence.61

As another court stated when faced with similar facts, "[i]t was the function and limitation of the cell-phone technology which motivated the investigating agents to conduct an immediate search of the phones, rather than seek a warrant."62

Other courts have agreed with this general line of reasoning that an exigency exists when officers search a cellular phone's contents. For example, the Northern District of West Virginia upheld a warrantless search of defendants' cellular phones that were seized during a search of their persons.63 The court examined the specific features of the phone at issue, finding that the Motorola V3 "Razer" had an automatic delete function by which an owner could set the phone to purge all text messages every one to ninety-nine days.64 According to the court, this feature created an exigency that justified officers' warrantless searches of the phones, because the text messages could have been lost as evidence.65

Thus where one court found that the limitation of cellular phone technology justified a warrantless search,66 another cited a phone's advanced feature in upholding a similar search.67 But whether a specific phone's technology is limited

61. Id.
64. Id. at *13.
65. Id.
or advanced may be irrelevant. First, cellular service providers keep records of incoming and outgoing calls,\(^\text{68}\) eliminating any exigency regarding the potential loss of phone numbers from the list of recent calls stored in a cellular phone. Text messages, however, present a more difficult issue, as cellular companies generally only store the contents of text messages on private accounts for about two weeks before deleting them.\(^\text{69}\) Still, if text messages are, in fact, saved for roughly two weeks, then it leaves officers more than adequate time to obtain a warrant and serve it upon the cellular company. In the case of government or company-issued phones, texts are often saved because of the legal requirements pertaining to business or government-related communications.\(^\text{70}\) Further, some text messages can be retrieved from a cellular phone’s Subscriber Identity Module (SIM) card even after the user has deleted them, as long as new information has not been stored over the old message.\(^\text{71}\)

One then must question where the exigency exists. The telephone numbers stored in a phone are certainly not lost, and text messages are feasibly accessible for about two weeks from the cellular provider and potentially for longer if they still exist on the SIM card. Further, address books contain

---

\(^{68}\) A cellular phone user for the past nine years, the author has received a statement every month listing all incoming and outgoing calls and text messages. This experience has been consistent among three separate cellular phone companies—Verizon, U.S. Cellular, and TMobile—during this time period. Therefore, it seems safe to assume that cellular companies do, in fact, retain records of incoming and outgoing calls and text messages. For an example of a court operating under the same assumption, see United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at *7 n.3 (E.D. Mo. Apr. 29, 2008) (“I am not convinced by the government’s evidence that even the call logs are in danger of being destroyed by incoming calls. The service provider keeps records of the incoming and outgoing calls . . . .”) (citation omitted).

\(^{69}\) See Mike Wendland, Mayor’s Texts Weren’t Private, but Yours Probably Are, USA TODAY, Jan. 24, 2008, http://www.usatoday.com/news/nation/2008-01-24-detroit-texts_N.htm. A spokesman for Sprint reportedly stated: We do keep [text messages] for about two weeks . . . . But that’s just to make sure they get sent if the customer’s phone is turned off or out of the network. After that, even if not retrieved, they’re gone. We don’t store them. We have no record of them. That’s standard practice in the industry.

\(^{71}\) See id.
static information that remains in the phone indefinitely. As one district court observed in a footnote:

There is no evidence that a cell phone's address book would be altered by incoming calls, and I am not convinced by the government's evidence that even the call logs are in danger of being destroyed by incoming calls. The service provider keeps records of the incoming and outgoing calls . . . , and so the fact that they might not all be stored on the phone itself does not mean they will be lost forever. To the extent that the government has cited cases holding otherwise, I disagree with the conclusions of those courts.\(^7\)

Therefore, courts that allow the search of a cellular phone's contents based on exigent circumstances may be furthering a legal fiction—that an exigency exists merely because the information that police seek is stored on a cellular phone, regardless of whether there is a true risk of losing the information. The simple fact that an item is a cellular phone does not alone create a "now or never" situation in which police must act immediately to preserve evidence of a crime.\(^3\) Therefore, unless a warrant exception other than the exigent circumstances doctrine applies, law enforcement officers should generally obtain a warrant before searching a cellular phone's contents.

### B. The Search Incident to Arrest Exception

Courts have more commonly upheld warrantless searches of cellular phones by means of the exception for searches incident to arrest. The Supreme Court has justified this warrant exception on the twin grounds of officer safety and preventing the destruction of evidence.\(^4\) Thus an officer, to

---


74. Chimel v. California, 395 U.S. 752, 763 (1969). As Justice Stewart explained for the Chimel majority:

[It] is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition,
prevent an arrestee from reaching a weapon to harm the
officer or effectuate an escape, may search the person of the
arrestee as well as the immediately surrounding area,
commonly called the "grab area." Likewise, an arresting
officer can search the arrestee and immediately surrounding
area for evidence that an arrestee could destroy or hide.

Courts allowing warrantless cellular phone searches
based on the search incident to arrest exception have
generally reasoned that a cellular phone differs little from a
basic pager, address book, or cigarette box, all which may be
lawfully searched incident to a suspect's arrest. These
courts' conclusions may be further justified by the notion that
a phone may contain evidence that a technologically swift
suspect could easily delete with the stroke of a key.
However, a minority of courts have struck down the search of
a cellular phone incident to arrest, differing significantly in
reasoning from the courts that have validated such searches.
This subsection lays out both arguments, finding that the
minority reflects a more constitutionally sound position.

Before examining courts' application of search incident to
arrest doctrine to cellular phone searches, this discussion
must consider two earlier cases: United States v. Robinson
and United States v. Chadwick. These cases provide the
ideological fork in the road by which courts have diverged on

it is entirely reasonable for the arresting officer to search for and seize
any evidence on the arrestee's person in order to prevent its
concealment or destruction. And the area into which an arrestee might
reach in order to grab a weapon or evidentiary items must, of course, be
governed by a like rule.

Id. 75. See id.; United States v. Gandia, 424 F.3d 255, 261–62 (2d. Cir. 2005)
(“Under Chimel, police may conduct a search of the arrestee's person and the
area within his immediate control—construing that phrase to mean the area
from within which he might gain possession of a weapon or destructible
evidence, i.e., the ‘grab area.’”) (internal citation and quotation marks omitted)).
One of the earliest courts to use the term "grab area" in an opinion was the
Court of Appeals of New York in People v. Clements, 339 N.E.2d 170, 178 (N.Y.
1975).

76. See Chimel, 395 U.S. at 763.
78. See Adam M. Gershowitz, The iPhone Meets the Fourth Amendment, 56
UCLA L. REV. 27, 40 (2008) (“An arrestee familiar with the functions of his cell
phone could just as easily delete text messages or call logs as he could tear up a
letter or an incriminating list of addresses on a piece of paper.”).
Robinson is famous for its holding that a defendant's cigarette box, found on his person, could be searched incident to his arrest.\textsuperscript{81} In Robinson, an officer arrested Willie Robinson for driving after his license had been revoked.\textsuperscript{82} The officer searched Robinson incident to the arrest and removed a crumpled cigarette package from his coat pocket.\textsuperscript{83} The officer then searched the contents of the cigarette package and found capsules containing heroin.\textsuperscript{84} The Court held that the search incident to Robinson's arrest lawfully extended to the illegal contents of the cigarette package.\textsuperscript{85}

Later, in Chadwick, the Court distinguished Robinson. There, police had seized a double-locked foot locker from a defendant's car and subsequently searched its contents at the police station more than an hour later.\textsuperscript{86} The Court cited Robinson in stating that, incident to an arrest, a search of items "within the 'immediate control' area" of the arrestee is generally reasonable.\textsuperscript{87} However, the Court distinguished between items that are immediately associated with the arrestee's person and other items, such as luggage:

Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.\textsuperscript{88}

In the reasoning of the Court, the foot locker was not immediately associated with the arrestee's person, and thus once police had exercised exclusive control over it and more than an hour had passed, the search was no longer incident to the arrest.\textsuperscript{89} Accordingly, the search was unreasonable absent a warrant.\textsuperscript{90}

\begin{itemize}
\item \textsuperscript{81} Robinson, 414 U.S. at 236.
\item \textsuperscript{82} Id. at 220.
\item \textsuperscript{83} Id. at 223.
\item \textsuperscript{84} Id.
\item \textsuperscript{85} Id. at 236.
\item \textsuperscript{86} United States v. Chadwick, 433 U.S. 1, 4 (1977).
\item \textsuperscript{87} Id. at 15 (citing Robinson, 414 U.S. 218).
\item \textsuperscript{88} Id.
\item \textsuperscript{89} Id.
\item \textsuperscript{90} See id. at 15–16.
\end{itemize}
Turning back to the cellular phone cases, courts have applied Robinson and Chadwick differently in reaching different outcomes. For instance, in United States v. Finley, the Fifth Circuit validated a warrantless cellular phone search incident to the defendant's arrest. There, officers seized the defendant's cellular phone, which was found on his person, incident to a drug arrest. Later, at another location, the officers interviewed the defendant, at which time they searched the phone's call records and text messages and questioned him about them. A number of the text messages related to narcotics dealings and were subsequently used in the prosecution. The court explained that a cellular phone, unlike the foot locker in Chadwick, "does not fit into the category of 'property not immediately associated with [his] person.'" Rather, the phone was more analogous to the cigarette box found in Robinson's coat pocket. Therefore, the court held that the search of the phone's contents did not violate the Fourth Amendment, as it was a valid search incident to arrest. A majority of courts facing similar facts have agreed with Finley's conclusion.

The court in United States v. Park, however, viewed things differently. In that case, officers did not seize or search the defendants' cellular phones at the time of arrest or soon thereafter. Rather, they first transported the defendants to the police station for booking, where they then seized the defendants' cellular phones and placed them into envelopes. Officers eventually searched the phones more

91. United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).
92. Id. at 254.
93. Id. at 254–55.
94. Id.
95. Id. at 260 n.7 (quoting United States v. Chadwick, 433 U.S. 1, 15 (1977)).
96. See id. at 260 (citing United States v. Robinson, 414 U.S. 218, 235 (1973)).
99. Id. at *2.
100. Id.
than ninety minutes after the arrests had occurred. The Park court held that the searches violated the defendants' Fourth Amendment rights, and thus the evidence was inadmissible. The court noted that Finley could be distinguished because there, the court found that the search was "substantially contemporaneous" with arrest, whereas the Park search occurred at the station house roughly an hour and a half after the arrest. However, it was not this factual difference, but rather a more fundamental ideological principle, upon which the court based its analysis. The court stated:

More fundamentally, however, this Court finds, unlike the Finley court, that for purposes of Fourth Amendment analysis cellular phones should be considered "possessions within an arrestee's immediate control" and not part of "the person." This is so because modern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.

Thus the phones, in containing potentially vast amounts of the most private information, were less comparable to Robinson's cigarette box and more like Chadwick's locked foot locker. Under Chadwick, once police had reduced the phones to their exclusive control and no exigency existed regarding destruction of evidence, they should have obtained

101. Id. at *1.
102. Id. at *7.
103. Id. at *7–8 (citing United States v. Finley, 477 F.3d 250, 260 n.7 (5th Cir. 2007)).
104. Some courts have distinguished or dismissed Park on the timing issue where officers have searched a phone contemporaneously with arrest. See United States v. Santillan, 571 F. Supp. 2d 1093, 1103 n.5 (D. Ariz. 2008); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008); United States v. Curry, Criminal No. 07-100-P-H, 2008 WL 219966, at *9 (D. Me. Jan. 23, 2008). However, the Park court made clear that the timing issue is not the foundation on which its difference with Finley rests. See Park, 2007 WL 1521573, at *8.
105. Park, 2007 WL 1521573, at *8 (internal footnotes omitted).
106. Id.
a warrant to search the contents of the phones.\textsuperscript{107}

Thus there exists a budding divide. Most courts have agreed with Finley's reasoning, interpreting Supreme Court case law to support warrantless cellular phone searches incident to arrest.\textsuperscript{108} These courts also find support in cases involving the search of pagers.\textsuperscript{109} Almost uniformly, courts have allowed the warrantless search of a pager's contents, and cases in the Finley camp often analogize pagers to cellular phones in upholding warrantless searches of cellular phones incident to arrest.\textsuperscript{110} However, the Park court refused to accept such a shaky analogy, recognizing the vast difference in the privacy interests at stake regarding cellular phones as compared to pagers.\textsuperscript{111} After all, traditional pagers contain only coding information, while cellular phones contain potentially vast amounts of content-based information. More basically, a small minority of courts to date has refused to accept further erosion of the Fourth Amendment's warrant requirement absent authoritative guidance.\textsuperscript{112} The Park court stated:

The Court recognizes that subsequent cases have extended Chimel's reach beyond its original rationales . . . . However, absent guidance to the contrary from the Ninth Circuit or the Supreme Court, this Court is unwilling to further extend this doctrine to authorize the warrantless search of the contents of a cellular phone—and to effectively permit the warrantless search of a wide range of electronic storage devices—as a "search incident

\textsuperscript{107} Id.


\textsuperscript{109} See, e.g., Finley, 477 F.3d at 260 (citing as analogous, United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (upholding search of pager incident to arrest)); Santillan, 571 F. Supp. 2d at 1102 (citing as analogous, United States v. Chan, 830 F. Supp. 531, 534–36 (N.D. Cal. 1993) (discussing search of a pager incident to arrest valid)); Ortiz, 84 F.3d at 984 (discussing whether the defendant had a reasonable expectation of privacy in the contents of the pager's memory)).

\textsuperscript{110} See supra note 109; Gershowitz, supra note 78, at 37.

\textsuperscript{111} Park, 2007 WL 1521573, at *9.

to arrest."\textsuperscript{113}  

It is this minority that has shown respect for basic Fourth Amendment principles and deference to the warrant requirement.

\textbf{C. Scope and Timing Issues}

One must also question whether traditional notions of the lawful scope of a search incident to arrest even fit in the cellular phone context. Recall that a search incident to arrest lawfully extends to the arrestee’s person and the immediately surrounding area. But traditional cases like \textit{Robinson} and \textit{Chadwick}, both addressing the scope of a search of physical evidence, may be a poor fit for cellular devices. With cellular phones, a different notion of scope is at play—virtual rather than spatial. The vast amount of information that may be stored digitally in a cellular phone far exceeds traditional concepts of the physical evidence that an arrestee can reach. This observation is magnified when one considers that many cellular phones can access remote databases. The virtual scope of a cellular phone’s contents is thus very different from the spatial scope of a defendant’s “grab area.” The \textit{Robinson/Chadwick} concept of scope concerns physical objects (illegal drugs in both cases), whereas the virtual concept of scope concerns digital information. This distinction may

\textsuperscript{113} \textit{Park}, 2007 WL 1521573, at *9. The court in \textit{United States v. Wall} similarly refused to extend the search incident to arrest exception to include cellular phones:

\begin{quote}
The Court declines to adopt the reasoning of Finley and extend law to provide an exception to the warrant requirement for searches of cell phones. The search of the cell phone cannot be justified as a search incident to lawful arrest . . . [T]he justification for this exception to the warrant requirement is the need for officer safety and to preserve evidence . . . . The content of a text message on a cell phone presents no danger of physical harm to the arresting officers or others. Further, searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant.
\end{quote}

\textit{Wall}, 2008 WL 5381412, at *3. The court in \textit{United States v. James} agreed in dicta:

\begin{quote}
I do not adopt [the Magistrate Judge's] conclusion that the search of the cell phone was also justified as a search incident to arrest. I recognize that the majority of cases considering this issue have concluded . . . that similar warrantless searches are proper . . . . I believe, however, that the analysis in \textit{United States v. Park} and \textit{United States v. LaSalle} is more consistent with the Fourth Amendment.
\end{quote}

\textit{James}, 2008 WL 1925032, at *10 n.4 (citations omitted).
indicate a difference in the motivation for these two different types of searches: whereas officers may be looking for contraband in a search for physical objects, they may be conducting evidentiary searches when accessing the digital information stored on a cellular phone. While the former is lawfully rooted in the prevention of evidence destruction, the latter is little more than a shortcut avoiding the longer route of obtaining a warrant for information not at risk of being destroyed. Where scope is virtual rather than spatial, the sheer volume of digital information available within what was traditionally considered a limited "grab area" raises new privacy concerns and requires a new articulation of the proper scope of a cellular phone's search incident to arrest.

Further, the Supreme Court's 2009 holding in Arizona v. Gant114 raised a timing issue for searches incident to arrest that could have widespread impact on searches of all containers, including cellular phones. In that case, Gant was arrested for driving while his license was suspended and subsequently handcuffed and placed in the back of a patrol car.115 While he was locked in the back of the patrol car, police searched his vehicle and found cocaine in a jacket on the back seat.116 The Court, with Justice Stevens writing the opinion, held that the search was invalid because "the Chimel rationale authorizes police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."117 This holding limited a common and broad reading of the rule of New York v. Belton, which held that officers, incident to a lawful arrest of a car's recent occupant, can search the entire passenger compartment of that car (and any containers inside) without a warrant.118

While the Gant Court does not discuss it much further, its holding focuses upon the proper point in time at which the

115. Id. at 1714.
116. Id.
117. Id. at 1719. The Court also held "that circumstances unique to the vehicle context justify a search incident to a lawful arrest when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" Id. (quoting Thornton v. United States, 541 U.S. 615, 632 (Scalia, J., concurring)). For purposes of this commentary on timing, this holding is not relevant.
118. Id. at 1717 (citing New York v. Belton, 453 U.S. 454, 460 (1981)).
scope of a search (at least of a car) incident to arrest should be measured.\textsuperscript{119} By holding that the search incident to arrest was improper since the arrestee was secured and not within reaching distance of the car, the Court measured whether the scope of the search was proper \textit{at the time of the search} rather than \textit{at the time of the arrest}.\textsuperscript{120} Further, it is difficult to see why measuring a search’s scope based on the time of search rather than the time of arrest should be limited to a scenario involving the search of an automobile incident to arrest. Should it not apply to a case like \textit{United States v. Brown}, where a pouch had been moved beyond the secured arrestee’s reach before it was searched?\textsuperscript{121} In \textit{Brown}, the D.C. Circuit upheld the search as a search incident to arrest, citing \textit{Belton} and stating that a search incident to arrest is valid as long as it is limited to “containers in hand or within reach when the arrest occurs.”\textsuperscript{122} But if courts going forward apply \textit{Gant}’s timing analysis generally to other searches incident to arrest, then an officer seizing an arrestee’s cellular phone would not be able to search the phone’s contents once the arrestee is secured and out of reach of the phone. In addition, many lower courts have explicitly applied \textit{Belton} to non-automobile contexts.\textsuperscript{123} It follows, then, that even if courts do not apply \textit{Gant}’s timing holding broadly to all searches incident to arrest, courts explicitly applying \textit{Belton} to non-automobile contexts should follow \textit{Gant}’s rule in these same non-automobile contexts.

The \textit{Gant} holding could be viewed as a straight application of \textit{Chadwick}. A car is “personal property not immediately associated with the person,” and thus once there is no longer a threat that a weapon could be seized from it or evidence inside it destroyed, “a search of that property is no longer an incident of the arrest.”\textsuperscript{124} \textit{Gant} does not look to upset searches of items “immediately associated with the person,” like the cigarette box in \textit{Robinson}, because these

\textsuperscript{119} See \textit{id.} at 1719.
\textsuperscript{122} See \textit{id.} at 587.
\textsuperscript{123} See, \textit{e.g.}, \textit{United States v. Tavolacci}, 704 F. Supp. 246, 252–53 (D.D.C. 1988) (citing cases applying \textit{Belton} to non-automotive factual scenarios).
items are easily distinguished from cars.\footnote{125} In the end then, the Robinson/Chadwick distinction regarding whether a cellular phone is an item “immediately associated with the [arrestee’s] person” or “personal property not immediately associated with the [arrestee’s] person” could become even more pivotal if courts apply \textit{Gant} outside the automobile context.\footnote{126} In the former scenario, \textit{Gant} would not apply; in the latter, \textit{Gant} would limit the search of a cellular phone incident to arrest to a situation where the arrestee is unsecured and still within reach of the phone.

\textbf{D. A New Standard for Searching Cellular Phones Incident to Arrest}

Although cellular phones potentially contain large amounts of private information, it is not clear that their search incident to arrest should be precluded altogether. The above analysis demonstrates that searches of cellular phones under the guise of exigent circumstances should generally not be allowed, at least as the exigency allegedly pertains to the loss of numbers from a recent call list or the loss of text messages.\footnote{127} Still, the wholesale prohibition of cellular phone searches incident to arrest could be too limiting.

One reason for allowing the continued search of cellular phones incident to arrest may be that some of the information, such as an address book and photographs, is the same kind of information that is often stored in a purse or a wallet. Why should officers be precluded from obtaining this information from a cellular phone but allowed to retrieve it from a wallet? One answer may be that the very fact that the information exists on a cellular phone, along with megabytes upon megabytes of pictures or other private information, places this “container” in its own category and precludes the obtaining of any information from it absent a warrant. This seems to be where the \textit{Park} court’s analysis leads, and it is the standard advocated by one recent commentator.\footnote{128}

\begin{footnotesize}
\begin{enumerate}
\item See generally \textit{Gant}, 129 S. Ct. 1710.
\item Of course, courts could easily confine \textit{Gant} to the automobile context if they desire, at least until the Supreme Court (if ever) more explicitly states that it applies to all search incident to arrest scenarios.
\item See \textit{supra} Part IV.A.
\item See Bryan A. Stillwagon, Note, \textit{Bringing an End to Warrantless Cell Phone Searches}, 42 GA. L. REV. 1165, 1201 (2008) (“[T]he first step in solving
\end{enumerate}
\end{footnotesize}
Conversely, Professor Gershowitz argues that "it . . . makes sense to allow police to review electronic call histories and text messages" because they could be easily deleted by an arrestee, just as papers in a wallet can be quickly destroyed. 129 While this argument is logical, it is tempered by two observations: (1) if officers have truly reduced a phone to their exclusive possession and there is no longer an exigency, then an arrestee could not feasibly destroy the information; 130 and (2) even if deleted from a phone, call histories and text messages are likely available from the cellular provider, and thus their "destruction" would not eliminate law enforcement's ability to obtain the information. 131

Another possibility lies in allowing the search of only a phone's coding information incident to arrest. This approach has the attractiveness of continuing the bright-line rule approach to search incident to arrest doctrine, but some might see it as still too limiting for law enforcement. It would allow officers to view recent call lists and text message addressees, but not the content of text messages, photos, or address books. With this rule, there would be less risk of law enforcement viewing the information for which there is a heightened expectation of privacy. Content-based information stored in mass quantity—and its highly private nature—is what puts cellular phones in a separate class from other containers. Prohibiting the viewing of a phone's content-based information while allowing officers to view its coding information could allow law enforcement to obtain information it frequently desires (e.g., call lists) while granting citizens a safeguard against free reign over their more personal information. Some courts have approved of this brand of distinction, allowing coding information to be admitted while suppressing content-based information. 132

the problem of warrantless cell phone searches is for the judiciary to recognize that cell phones are, in fact, much more analogous to modern computers than to wallets, briefcases, or even pagers, and thus 'police should obtain a search warrant, just as they would when they seize a personal computer from an accused.'" (quoting State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *10 (Ohio Ct. App. July 25, 2008) (Donovan, J., dissenting)).

129. See Gershowitz, supra note 78, at 40.
130. See Gant discussion, supra notes 114–26 and accompanying text.
131. See supra Part IV.A.
132. As one court stated:

Moreover, we note that the trial court permitted only evidence pertaining to the cell phone's call record and numbers matching those
Still another option lies in allowing a search incident to arrest of all the information stored on a phone, while disallowing a search that accesses information stored on remote databases. This would allow officers to search a phone's text messages, call records, address book, and photographs, while forbidding them from listening to voicemails (or viewing emails, for phones with this capability), which are generally stored on remote servers. This is one approach offered by Professor Gershowitz, and it does improve upon the current jurisprudential general trend that would seemingly allow the search of all of a phone's contents in addition to remotely accessed data. However, this approach leaves too much private information unprotected from a search incident to arrest. If courts adopted this rule, it would subject anyone who is the subject of a custodial arrest, even for a traffic violation, to a pre-approved foray into a virtual warehouse of their most intimate communications and photographs without probable cause.

A prohibition on searching cellular phones incident to arrest, as the Park court essentially ruled, is a feasible reading of Supreme Court precedent and respects basic Fourth Amendment protections against unreasonable searches. In addition, as discussed above, application of the

supplied by the informant . . . . It granted, however, [the defendant's] motion to suppress incriminating photos also retrieved by the officers from the phone. In doing so, the court appropriately admitted only that evidence which the officers had a reasonable suspicion was on [the defendant's] person at the time of his arrest. Thus, the broader privacy concerns addressed in Park were not implicated here.


133. At least one court has upheld the search of a camera incident to arrest, which would support this view in terms of the photographs viewed while searching a cellular phone. See United States v. Ayalew, 563 F. Supp. 2d 409, 416 (N.D.N.Y. 2008).

134. See Gershowitz, supra note 78, at 56. Gershowitz observes that courts "almost certainly will . . . . apply the search incident to arrest doctrine to the iPhone," potentially allowing officers to view an iPhone's photos, movies, recently viewed websites, emails, and a host of other information. Id. at 44.

Gant holding to this context would buttress the Park rationale, disallowing such searches if the arrestee were secured and out of reach of the cellular phone. However, courts are unlikely to follow the lead of Park and the minority, at least if they distinguish Gant as inapplicable outside the automobile context. In light of this reality, the coding/content-based distinction is a reasonable compromise and a workable option. It is a clear, relatively bright-line rule, which courts prefer in the search incident to arrest context. It protects citizens' Fourth Amendment privacy rights while still giving law enforcement much of what it already seeks (i.e., call and text message coding information). This approach does limit police from immediately obtaining a significant amount of information, but there is a minimal risk of losing this content-based data, and it can be acquired with a warrant. The coding/content-based distinction also establishes a reasonable limiting line regarding the virtual scope of a search of digital information incident to arrest. Where traditional notions of physical scope are a poor fit for digital information, this distinction provides a virtual "grab area" within which law enforcement could legally operate.

Distinguishing between coding and content-based data may be a more appropriate solution than an all-out ban on searching cellular phones incident to arrest because the custodial arrest context does justify a "reasonable intrusion" into an arrestee's belongings. Admittedly, such a distinction could prove a bit messy, as officers may, at times, inadvertently view content-based information while searching only for coding information. Further, this type of scenario might lead to difficult fact-finding in suppression hearings; but fact-finding in suppression hearings is often difficult, and this difficulty alone should not be enough to discard a workable rule. There must be a line at which an intrusion becomes unreasonable despite a custodial arrest. Protecting a phone's practical library of private communications and

136. See Gershowitz, supra note 78, at 39, 40.
137. Id. at 34 (noting the "Court's affinity for bright-line rules").
138. See United States v. Robinson, 414 U.S. 218, 235 (1973) ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification . . . . It is the fact of the lawful arrest which establishes the authority to search.").
photographs from limitless viewing is an appropriate line. The coding/content-based distinction establishes this line, and it is a standard that courts and legislators should implement.

V. "SMART PHONES"

Technology and the Fourth Amendment continue to grapple as advances in technology persist. Recently, cellular phones have morphed into something far more complex. In turn, new Fourth Amendment questions accompany the advent of such devices as the iPhone, G2, and multiple varieties of the Blackberry, as what were once phones are now instruments comparable to computers.\textsuperscript{139}

Like computers, smart phones allow a user to access the Internet, share photographs, view movies, and use email, among other functions.\textsuperscript{140} Some smart phones add to this list the ability to record and replay live video,\textsuperscript{141} a capability that many computers lack. While they still serve as phones, telephonic capability alone no longer limits an electronic device's identity to that of a phone alone. After all, some people now use their personal computers and laptops instead of phones, communicating orally through services like Skype.\textsuperscript{142} Difficulty lies in defining what exactly distinguishes a smart phone from an older generation phone. No agreement looks to exist regarding what exactly qualifies as a so-called smart phone, and what does not.\textsuperscript{143} It could be built-in email capability that sets a device apart as a smart phone, or the running of a full operating system, or maybe a touch screen or a full keyboard. It is safe to say, however, that the more a cellular device operates like a full-fledged computer, the "smarter" it is. This section later revisits the question, seeking a workable definition of "smart phone" that

\begin{footnotesize}
\begin{enumerate}
\item As one court has observed, "[a] cell phone is similar to a personal computer that is carried on one's person." United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008).
\item David Pogue, A Blackberry with No Keyboard?, N.Y. TIMES, Nov. 27, 2008, at B1.
\item For a sampling of a variety of smart phones and an example of the lack of popular agreement on how to define the term, see Smart Phone, WIKIPEDIA, http://en.wikipedia.org/wiki/Smartphone (last visited June 6, 2008).
\end{enumerate}
\end{footnotesize}
can be quickly and easily determined.

The reality that these newer devices function more like computers than simple phones raises questions. Should they be treated like any other cellular phone that is searched incident to arrest? Or are these devices of such a unique and complex character that they have moved beyond what may reasonably be considered a cellular phone? Might the potential for storing seemingly endless amounts of the most private information place these instruments in a different category of Fourth Amendment jurisprudence?

A. Searching Computers Incident to Arrest

The capabilities of these new cellular devices create concerns beyond whether law enforcement is able to view call lists, address books, and even text messages. As the Park court stated in excluding evidence obtained from a cellular phone incident to arrest:

Any contrary holding could have far-ranging consequences. . . . [T]he government asserted that, although the officers here limited their searches to the phones’ address books, the officers could have searched any information—such as emails or messages—stored in the cell phones. In addition, in recognition of the fact that the line between cell phones and personal computers has grown increasingly blurry, the government also asserted that officers could lawfully seize and search an arrestee’s laptop computer as a warrantless search incident to arrest. As other courts have observed, “the information contained in a laptop and in electronic storage devices renders a search of their contents substantially more intrusive than a search of the contents of a lunchbox or other tangible object. A laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records.”

One then must analyze not only whether traditional cellular phones are searchable incident to arrest, as discussed prior, but also whether laptops or personal computers are

searchable incident to arrest. This subsection focuses solely on the search incident to arrest exception as applied to the search of computers, and not on the exigent circumstances exception, because smart phones' computer-like characteristics do not change the exigent circumstances discussion from Part IV.A of this article. The same exigent circumstances analysis for older generation phones applies to smart phones: cellular service providers keep records of the information at risk of being lost, and thus no real exigency exists. Smart phones' comparability to computers, however, bears upon whether they are searchable incident to arrest—if smart phones and computers are synonymous, then the same rule should apply to both.

A search of case law turns up a paucity of precedent regarding the search of laptops or other computers incident to arrest. It is unclear why there are so few cases involving searches of computers incident to arrest. Computers have been around for decades now, and laptops for many years as well. Yet no federal cases and only one state case have assessed the validity of a computer search incident to arrest. The answer may be that even police do not believe a search of a computer incident to arrest is permissible, seeking instead a warrant for the search of computers. One may look to the plethora of case law discussing the search of computers pursuant to warrants in support of this answer. Granted,

145. This section considers only the search incident to arrest exception to the warrant requirement. It is the most common exception applied to warrantless cellular phone searches, and the most problematic considering it requires no articulable suspicion at all, much less probable cause.


147. See, e.g., United States v. Cartier, 543 F.3d 442 (8th Cir. 2008); United States v. Henderson, 536 F.3d 776 (7th Cir. 2008); United States v. Giberson, 527 F.3d 882 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008); United States v. King, 509 F.3d 1338 (11th Cir. 2007); United States v. Rayburn House Office Bldg., Room 2113, 497 F.3d 654 (D.C. Cir. 2007); United States v. Flanders, 468 F.3d 269 (5th Cir. 2006); Armstrong v. City of Melvindale, 432 F.3d 695 (6th Cir. 2006); United States v. Martin, 426 F.3d 83 (2d Cir. 2005); Bellville v. Town of Northboro, 375 F.3d 25 (1st Cir. 2004); United States v. Zimmerman, 277 F.3d 426 (3d Cir. 2002); Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001).

Further highlighting law enforcement's focus on obtaining warrants to search computers, many jurisdictions give explicit instructions on how to effectively articulate the description in a warrant when seeking to obtain
computers are often located in homes and the subject of an investigation, leading to more necessity and incentive for police to obtain a warrant. However, it is not uncommon for people to carry laptops wherever they go, whether in the car, on a train, at the airport, or at a coffee shop. Considering the commonality of laptops, what else explains the utter lack of cases applying search incident to arrest doctrine but law enforcement's general assumption that a warrant is needed to search an individual's computer? Courts have also applied other warrant exceptions to computer searches, although these instances are still few in number. Therefore, one can start at a minimum with the assumption that the warrantless search of a computer incident to arrest is legally unprecedented and thus questionable at best.

The Court of Appeals of Washington is the only court that has addressed the legality of a search of a computer incident to arrest. In *State v. Washington*, police arrested the defendant on suspicion of auto theft. Incident to the arrest, an officer observed a black bag on the floor of the car. The officer unzipped the bag and discovered a laptop inside, which the defendant stated he had bought for fifty dollars. The officer brought the laptop to the station on the suspicion that it was stolen, and another officer searched it to determine the identity of its lawful owner. The court held that the arrest was based upon probable cause and that the search of the bag was “proper as a search incident to arrest.” However, although the police had probable cause to seize the laptop, the “subsequent search of the computer’s files . . . did not fall under any of the exceptions to the warrant requirement.” Therefore, the court held that the evidence obtained from the laptop should have been suppressed. Thus, since it applied

---

150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.* at *3.*
154. *Id.*
the search incident to arrest exception to the search of the bag but held that no warrant exception applied to the laptop's search, the court made it clear that the laptop could not be searched incident to the defendant's arrest.\textsuperscript{156}

Other cases have discussed in dicta the legality of a computer search incident to arrest. The \textit{Park} court expressed worry that allowing the search of a cellular phone incident to arrest would lead to the search of laptops incident to arrest.\textsuperscript{157} It chose not to begin the journey down that road of Fourth Amendment erosion. Further, in \textit{United States v. Urbina}, Magistrate Judge Goodstein of the Eastern District of Wisconsin, while recommending upholding the search of a cellular phone incident to arrest, alluded that the search of a computer incident to arrest would be invalid:

[T]he court acknowledges the observations by the court in \textit{Park} that the line between a cell phone and a personal computer is becoming increasingly blurred. Many cell phones are capable of browsing the internet or sending and receiving email just like a personal computer. Certainly, there may be many instances where the text of emails sent and received, or a list of the websites a person visited, may be of interest to law enforcement. However, whether or not law enforcement may be permitted to access these records by virtue of the fact that an arrestee happened to have his cell phone on his person at the time he was arrested is a question not presented in this case. In the case before this court, it is clear that [the detective] limited his search to the phone's address book and call history. If the evidence in a future case were to show that the warrantless search conducted by law enforcement was \textit{essentially equivalent to a search of a personal computer}, without sufficient exigencies to justify such a search, the court's reaction may be different, because of the \textit{substantial invasion of privacy}.\textsuperscript{158}

\textsuperscript{156} See \textit{id. at *2–3}. The facts of the case do not disclose the length of time between the seizure of the laptop and its search at the station house. The court, in not discussing it, does not seem to concern itself with this detail. One might determine that the court never considered the search incident to arrest exception in relation to the laptop because it so clearly did not apply in the mind of the court.


Thus the court not only implied that it would invalidate the search of a computer incident to arrest, but it also found the fact that the officer limited the search of the phone to its address book and call history worth noting.

Another source of guidance lies in a case that applied the border exception to the warrant requirement—an exception that is distinctly different from the search incident to arrest exception. As the Supreme Court has stated, “the expectation of privacy is less at the border than it is in the interior.” At the nation’s border, law enforcement may search people and their belongings freely without any suspicion. Only where searches are highly intrusive, such as body cavity searches, is reasonable suspicion required. Yet even in this context of such a limited expectation of privacy, in United States v. Arnold, Judge Dean Pregerson of the Central District of California raised concerns similar to those that the Park and Urbina courts expressed. Although subsequently reversed by the Ninth Circuit, the district court invalidated the suspicionless search of an individual’s laptop computer, which was removed from the defendant’s luggage in the customs area of Los Angeles International Airport. The court explained that “opening and viewing confidential computer files implicates dignity and privacy interests. Indeed, some may value the sanctity of private thoughts memorialized on a data storage device above physical privacy.” At least one circuit court has also indicated that the search of a laptop at the border may not be “routine,” thus requiring reasonable suspicion. These instances, though limited to the border search context, are meaningful in that they support a general

160. Id. at 152.
161. See United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); United States v. Lawson, 461 F.3d 697, 700 (6th Cir. 2006); United States v. Braks, 842 F.2d 509, 511–13 (1st Cir. 1988).
163. Id. at 1000.
164. Id. at 1003 (citing United States v. Molina-Tarazon, 279 F.3d 709, 716 (9th Cir. 2002) (noting that “government intrusions into the mind” deserve equal protection as do physical intrusions), abrogated by United States v. Flores-Montano, 541 U.S. 149 (2004)).
165. See United States v. Roberts, 274 F.3d 1007, 1012 (5th Cir. 2001) (upholding a laptop search because it was based upon reasonable suspicion while assuming it was not “routine” in the border context).
notion that information stored on a computer is highly private, more so than most other information. For courts to suggest that computers may have a level of heightened privacy at the border, where Fourth Amendment protections are at their lowest level, speaks to the inherent level of privacy that attaches to computers.

Taken together, the lack of any meaningful case law applying search incident to arrest doctrine to computer searches, paired with the plethora of cases analyzing the legality of computer searches pursuant to warrants, indicate a general assumption that computers should not be subject to warrantless and suspicionless searches incident to arrest. This notion is buttressed by decisions such as Washington, Park, Urbina, and, presumably, United States v. James, which would exclude evidence obtained from the search of a computer incident to arrest. Finally, the suggestion of one court that a heightened level of privacy attaches to computers during border searches only strengthens the argument that computers should not be searched incident to arrest. The capacity for storing immense amounts of intimately private information simply places computers in a different category than other "containers."

B. A Different Standard for Computers and Their New Equivalents

If it is true that laptops and other computers are not searchable incident to arrest, then it necessarily follows that neither are smart phones (or at least they should not be). These devices are laptops’ new equivalents. As Professor Gershowitz has suggested, courts should not apply "an ill-fitting bright-line rule" to the iPhone and its peers. Unlike searches conducted with technology held by police, such as thermal imaging devices and helicopters, searches of smart phones—which are owned by private citizens en masse—have the potential to subject millions of people to rummages through their most private information without a hint of suspicion. Thus, if the warrantless search of a smart phone

167. See supra notes 155–58 and accompanying text.
168. Gershowitz, supra note 78, at 46.
169. See id. at 48. I do not wish to suggest that law enforcement officers
incident to arrest is a Fourth Amendment violation, then these searches have the potential to violate the Constitution on a mass scale.

Further, searching smart phones incident to arrest could be considered an end-run around the Fourth Amendment. If smart phones are in fact equivalent to computers, which police likely need a warrant to search, then searching smart phones incident to arrest is a shortcut to obtaining the desired data. But while it is less efficient to obtain a warrant, efficiency does not justify Fourth Amendment violations. Arguing that smart phones are more like older generation cellular phones than computers would be disingenuous in this light.

Gershowitz has suggested the following solutions to the problem of smart phones: (1) limiting searches incident to arrest to the crime related to the arrest, (2) encouraging state legislatures to enact more protective laws, (3) limiting searches of these devices to the applications that are open when the device is seized, (4) limiting searches of these devices to “five steps” of searching, and (5) distinguishing between data stored on the device and remote data accessible generally wish to violate privacy rights or aimlessly sift through the private information of citizens. However, unchecked authority in any forum naturally leads to abuses.

171. Gershowitz, supra note 78, at 49; see also Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring). This limitation was officially adopted by the Court in Gant, at least in the context of vehicle searches incident to arrest. Arizona v. Gant, 129 S. Ct. 1710, 1719 (2009) (“[C]ircumstances unique to the vehicle context justify a search incident to a lawful arrest when it is ‘reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.’” (citing Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring))).
172. Gershowitz, supra note 78, at 50–53.
173. Id. at 53–54.
174. Id. at 54–56. Here, Gershowitz suggests a “‘five-level deep’ rule (or some other admittedly arbitrary number) limiting the search of iPhones to a total of five steps.” Id. at 55. An example of this rule’s operation in the context of an iPhone would allow an officer to:

1. turn on the phone;
2. open the internet browser;
3. type in a web-based email account such as www.hotmail.com;
4. log into the account (if the user id and password are saved); and
5. open a folder of messages. If the officer completes the fifth step without finding anything incriminating that could be destroyed, the officer would need to stop searching. To search further, the officer would need to procure a warrant.

Id.
via the device. Gershowitz rightly notes that “despite the flaws associated with each proposal, all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant.” But he does not advocate altogether eliminating searches of iPhones and their progeny incident to arrest.

While these suggestions are creative and practical to varying degrees, each one falls short of appropriate Fourth Amendment protection if iPhones and their counterparts are truly akin to computers. Whatever rule applies to computers should certainly apply to new generation cellular devices, and a suspicionless search incident to arrest does not pass muster.

Therefore, a different rule should apply to smart phones as opposed to older generation cellular phones, and it should mirror the rule that applies to the search of a computer incident to arrest: a warrant is required. A lesser standard

175. Id. at 56–57.
176. Id.
177. As Gershowitz states:

Much as the traditional search incident to arrest cases permit police to open a wallet, take out a letter, and read it before the arrestee has an opportunity to destroy the evidence, it also makes sense to allow the police to review electronic call histories and text messages in a cell phone.

Id. at 40.
178. After all, courts have even invalidated the search of computers pursuant to warrants when officers have gone beyond a warrant’s scope. See, e.g., United States v. Carey, 172 F.3d 1268, 1275–76 (10th Cir. 1999) (discussing a holding officer who violated Fourth Amendment when he viewed numerous computer files pursuant to warrant without using the computer’s search function to limit the scope of what he viewed). The Carey court recognized that “[r]elying on analogies to closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.’” Id. at 1275 (quoting Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 HARV. J.L. & TECH. 75, 104 (1994)).

179. Some may argue that warrant exceptions based on probable cause, such as the automobile exception, should apply as well. I do not agree with this proposition because of the heightened privacy that attaches to a computer as opposed to other containers. But see United States v. Johnson, 495 F.3d 536, 543 (7th Cir. 2007) (holding probable cause search of a computer valid under the inevitable discovery exception).

For an example of appropriate police conduct regarding the search of an iPhone, see United States v. Lemke, Criminal No. 08-216(1) (DWF/RLE), 2008 WL 4999246, at *7 (D. Minn. Nov. 19, 2008). There, police seized the defendant’s iPhone pursuant to his arrest. Id. They then prepared an affidavit and secured a warrant before searching the contents of the phone for illegal
would allow the search incident to arrest exception to smother much of the protection the Fourth Amendment guarantees regarding private information stored on these devices. Further justifying a different rule for smart phones, the coding/content-based standard proposed for older generation phones in Part IV of this article would not work for these newer devices. Take, for instance, the iPhone. On that device, one can leave the photo function open when turning the phone off, so that when it is later turned on, that function is the first image that appears. This feature would make content-based information (photographs) immediately observable once the iPhone is powered on, requiring officers later to explain why they observed otherwise off-limits information in plain view. Such a scenario would lead to difficult fact-finding in suppression decisions, straying far from the Court's preferred bright-line search incident to arrest jurisprudence.\footnote{180. Thanks to Professor Gershowitz for helping flesh out this point. While difficult fact-finding in suppression decisions may not be reason alone to disregard a rule, in the context of smart phones, fact-finding difficulties are not the core reason the coding/content-based distinction is inappropriate. Rather, it is the fact that smart phones are synonymous with computers that drives the need for a different standard.}

Considering that two different rules are proposed in this article—one for older generation cellular phones and one for smart phones—an easily ascertainable line of distinction must be made if the rules are to work. While other lines of demarcation certainly exist, considering the technology as it stands today, the most workable distinction may be phones that have either a touch screen or a full keyboard. Older generation cellular phones, as defined here, do not have either of these two advanced features, while all smart phones referenced here (iPhones, G2s, and Blackberries) have either a touch screen or a full keyboard. Further, determining whether a phone has either a touch screen or a full keyboard would prove remarkably easy for officers: all one needs to do is look at the exterior of the phone to determine whether it holds one of these two features. As phones generally become more advanced, it seems that more will have either a touch screen or full keyboard. If this development occurs, then a

\footnote{Id. Such investigatory restraint is commendable and appropriate, and it should be the standard rather than the exception.}
new distinction would not be necessary. Rather, more devices would be protected against warrantless searches incident to arrest.

CONCLUSION

The new frontier of Fourth Amendment jurisprudence continues to expand as technology advances. This constant expansion creates difficulty for courts in applying decades-old case law to factual scenarios never before considered. One important challenge in the criminal procedure context involves the warrantless search of cellular phones by law enforcement.

Courts in recent years have regularly applied the warrant requirement’s exigent circumstances and search incident to arrest exceptions when analyzing the legality of searching cellular phones. The courts that have applied the exigent circumstances exception have established a developing legal fiction that information is at a high risk of loss merely because it exists on a cellular phone. These courts ignore the reality that most information stored on a cellular phone will remain there long enough for a warrant to be secured and that numbers “lost” from recent call lists are readily obtainable from the service provider. The courts that have applied the search incident to arrest exception have generally upheld cellular phone searches. A minority of courts applying this exception, however, has held that cellular phones are outside the ambit of the exception’s reach because of their capacity for storing vast quantities of intimately personal data.

Older generation cellular phones, which are less comparable to computers than newer devices like iPhones, still warrant heightened protection because of their capability for storing very large amounts of private data. For these phones, a workable standard (and worthwhile compromise to consider) for searches incident to arrest would allow officers to view coding information while prohibiting them from viewing content-based information. Any search of the content-based information of older generation phones would require a warrant or a probable cause warrant exception.

Smart phones, defined here as phones containing either a touch screen or full keyboard (e.g., iPhones, G2s, and Blackberries), are far more advanced than older generation
cellular phones. Further, they cannot be logically distinguished from laptops or other computers in terms of their functionality and capacity for information storage. Therefore, the standard for searching smart phones should be the same standard that applies to laptops and other computers. Although there is a dearth of search incident to arrest jurisprudence regarding laptops or personal computers, various factors indicate that many courts would invalidate such searches. Likewise, courts should invalidate the warrantless search of a smart phone if the only basis for the search is that it was incident to arrest. For computers and smart phones alike, courts should require that police obtain a warrant before examining the contents of these devices.

Courts may well continue to allow warrantless searches of cellular phones without adopting protective limits. Such a course would continue the expansion of the search incident to arrest exception, and it would further the erosion of the warrant requirement. If courts instead seek to uphold basic Fourth Amendment guarantees, however, they must guard against this potential for widespread intrusion into the privacy of the citizenry by adopting new standards for searches of cellular devices. These standards must be workable, logical, and most importantly—constitutional.

181. See Wayne A. Logan, An Exception Swallows a Rule: Police Authority to Search Incident to Arrest, 19 YALE L. & POL’Y REV. 381, 383 (2001) (“Like other exceptions, . . . the search incident exception has evolved to swallow the rule, so much so that the parameters and rationales originating the exception are now only vaguely recognizable in many decisions of courts across the land.” (citing California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring))); Stephen Gibbs, Note, In Search of Straightforward Rules: The Burger Court’s Expansion of the Search Incident to Arrest Exception to the Warrant Requirement, 22 SANTA CLARA L. REV. 1087, 1088 (1982) (“The prevalence of the search incident to arrest exception and its insulation from judicial examination indicates that the exception has, in reality, replaced the warrant requirement of the fourth amendment.”).

182. See Acevedo, 500 U.S. at 582 (Scalia, J., concurring) (describing the warrant requirement as “unrecognizable” because it has become “riddled with exceptions”). Rather than steadily eroding, the warrant requirement “has ridden something of a legal roller coaster,” passing through multiple periods of reverence and contempt over time. James J. Tomkovicz, California v. Acevedo: The Walls Close in on the Warrant Requirement, 29 AM. CRIM. L. REV. 1103, 1104 (1992). As a result of stark ideological opposition between the requirement’s supporters and its detractors, “the warrant tide has ebbed and flowed” in correlation with the changing face of the Supreme Court over the years. Id. at 1105.