2013

Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest

Sara M. Corradi

Follow this and additional works at: https://scholarlycommons.law.case.edu/caselrev

Part of the Law Commons

Recommended Citation
Sara M. Corradi, Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, 63 Case W. Rsrv. L. Rev. 943 (2013)
Available at: https://scholarlycommons.law.case.edu/caselrev/vol63/iss3/9

This Comments is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Law Review by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.
— Comment —

BE REASONABLE!

LIMIT WARRANTLESS SMART PHONE
SEARCHES TO GANT’S JUSTIFICATION
FOR SEARCHES INCIDENT TO ARREST

INTRODUCTION

Imagine that police officers arrest Robert White after an informant bought an ounce of cocaine from him. While searching Robert incident to his arrest, the police find his smart phone. In order to determine if Robert is working with any conspirators to sell the cocaine, the officers decide to search the contents of his phone, and come across photographs implicating him in a child pornography ring. Before trial on the charges of possession and distribution of child pornography, Robert moves to suppress the evidence found on his cell phone because officers searched it without a warrant.


2. This Comment uses the term smart phone to specify the modern cell phones defined by Encyclopedia Britannica. Id. When this Comment discusses cell phones, the term encompasses both smart phones and traditional cell phones, which simply send text messages and make

Conclusion
The above situation has become more common due to the heightened prevalence of smart phones in the United States. As such, courts have increasingly been required to determine the legality and parameters of cell phone searches—often coming to vastly different outcomes. Without proper guidance from courts, officers struggle to determine whether they may search, when they may search, and what information on the phone they may search. This Comment proposes a workable standard that should be uniformly followed by courts in order to provide guidance to officers as to when they may properly search a smart phone incident to arrest. Part I studies the history of the search incident to arrest exception to the warrant requirement. Part II surveys the different pathways lower courts used when analyzing cell phone searches. Part III examines two recent Supreme Court cases’ effect on the search of smart phones. Part IV defines the standard all courts should apply—and officers should follow—in determining if a search of a smart phone is lawful under current Supreme Court precedent. Overall, this Comment concludes that the reasoning set forth in the Supreme Court’s decision of Arizona v. Gant protects a smart phone from being searched incident to every arrest.

I. History of the Search Incident to Arrest Exception

The Fourth Amendment states that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .” Although the Supreme Court has often stated that warrantless searches are per se unreasonable, the Court has created many phone calls without the additional capabilities of a smart phone. The discussion of prior case law, in Part II, is an exception to this rule since many courts did not distinguish if the cell phone at issue was a smart phone or not.

3. See Katz v. United States, 389 U.S. 347, 357 (1967) (stating that warrantless searches are per se unreasonable).


5. See infra Part II.


7. U.S. Const. amend. IV.

8. See, e.g., Gant, 556 U.S. at 338 (stating that “searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment” (quoting Katz, 389 U.S. at 357)); California v. Carney, 471 U.S. 386, 401 (1985) (same).
exceptions. Each court to confront the issue of a warrantless cell phone search has analyzed the issue utilizing a different framework under the search incident to arrest theory of warrantless searches.

The search incident to arrest exception to the warrant requirement, which has developed through several Supreme Court opinions, permits officers to search a person and his effects upon valid arrest in order to protect police and to find evidence to use for prosecution. As early as 1914, the Supreme Court, in dicta, authorized officers “to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.” Several years later, the Court elaborated on this permission and stated that “[w]hen a man is legally arrested for an offense, whatever is found upon his person or in his control which it is unlawful for him to have and which may be used to prove the offense may be seized and held as evidence in the prosecution.” Only a few months later, the Court, again in dicta, stated that officers may search the place where a lawful arrest is made in order to search for evidence and weapons, and this was later used to uphold the search of a closet pursuant to a lawful arrest. In the years following the expansion of this policy, the Court swayed between permitting full searches of the premises where an arrest occurs and invalidating such searches.

9. See, e.g., Arizona v. Hicks, 480 U.S. 321, 326 (1987) (“It is well established that under certain circumstances the police may seize evidence in plain view without a warrant.” (quoting Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971))); Carroll v. United States, 267 U.S. 132, 153 (1925) (“[T]he guaranty of freedom from unreasonable searches and seizures by the Fourth Amendment has been construed . . . as recognizing a necessary difference between a search of a store, dwelling house or other structure in respect of which a proper official warrant readily may be obtained, and a search of a ship, motor boat, wagon or automobile, for contraband goods, where it is not practicable to secure a warrant because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.”).


12. Agnello v. United States, 269 U.S. 20, 30 (1925) (“The right without a search warrant contemporaneously to search persons lawfully arrested while committing crime and to search the place where the arrest is made in order to find and seize things connected with the crime as its fruits or as the means by which it was committed, as well as weapons and other things to effect an escape from custody, is not to be doubted.”).

13. See Marron v. United States, 275 U.S. 192, 199 (1927) (“They had a right without a warrant contemporaneously to search the place in order to find and seize the things used to carry on the criminal enterprise . . . The closet in which liquor and the ledger were found was used as a part of the saloon.”).

14. Compare Go-Bart Importing Co. v. United States, 282 U.S. 344, 358 (1931) (invalidating a search of the arrestee’s office), and United States
Finally, in 1969, the Court, in *Chimel v. California*, clarified its position on what searches an officer is permitted to conduct incident to arrest.\(^{15}\) In 1965, officers arrested Chimel pursuant to a warrant for burglary of a coin shop.\(^{16}\) Upon execution of the arrest warrant, the officers sought permission to search his house, which Chimel refused.\(^{17}\) Officers proceeded to search his entire home anyway, on the basis of the lawful arrest, and opened drawers and moved aside items to find evidence of the burglary.\(^{18}\) The Court held that

> [w]hen an arrest is made, 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. . . . In addition, 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.\(^{19}\)

The Court went on to state that “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.”\(^{20}\) Pursuant to these twin rationales of officer safety and evidence preservation, officers were no longer permitted to search the entire premises at which a person was arrested—they were limited to searching the arrestee himself and the area into which the arrestee might be able to reach.

In *United States v. Robinson*, the Court expanded the rule put forth in *Chimel*, holding that officers may search closed containers found on a person, or within his control, as a valid search incident to arrest.\(^{21}\) Officers arrested Robinson for driving with a revoked license and proceeded to search his person.\(^{22}\) The officer conducting

\(^{16}\) Id. at 753.
\(^{17}\) Id.
\(^{18}\) Id. at 754.
\(^{19}\) Id. at 762–63.
\(^{20}\) Id. at 763.
\(^{22}\) Id. at 220–22.
the search felt an object in Robinson’s pocket but could not determine what the object was, so he reached inside and pulled out a cigarette package.\textsuperscript{23} The officer testified that he was unsure what was inside the package, but could ascertain that it was not cigarettes, so he opened it to find fourteen capsules of heroin.\textsuperscript{24} The Court held that, “having in the course of a lawful search come upon the crumpled package of cigarettes, he was entitled to inspect it.”\textsuperscript{25} The Court held that it was not necessary to litigate in every case whether or not the officers were acting based on the theories of officer safety or evidence preservation since searching incident to arrest is reasonable under the Fourth Amendment.\textsuperscript{26}

The Court’s holding in \textit{Robinson} was subsequently used to justify a warrantless search of a closed container in an automobile incident to arrest. In \textit{New York v. Belton}, police stopped a vehicle for travelling at excessive speed and immediately smelled marijuana and saw an envelope on the vehicle’s floor related to marijuana use.\textsuperscript{27} After arresting all four men in the vehicle, the officer searched the vehicle.\textsuperscript{28} The officer found a jacket on the back seat, belonging to Belton, and proceeded to unzip the pockets, where he discovered cocaine.\textsuperscript{29} The Court held that police officers may search the passenger compartment of a vehicle incident to a lawful arrest and in doing so, officers may search any container found therein.\textsuperscript{30} In a footnote, the Court defined a ‘container’ as “any object capable of holding another object . . . includ[ing] closed or open glove compartments, consoles . . . luggage, boxes, bags, clothing, and the like.”\textsuperscript{31} According to the Court, it is not any reduced expectation of privacy that authorizes this search, but instead the lawful arrest justifies infringement on an arrestee’s privacy.\textsuperscript{32}

\textsuperscript{23} \textit{Id.} at 223.
\textsuperscript{24} \textit{Id.}
\textsuperscript{25} \textit{Id.} at 236.
\textsuperscript{26} \textit{Id.} at 235.
\textsuperscript{28} \textit{Id.} at 456.
\textsuperscript{29} \textit{Id.}
\textsuperscript{30} \textit{Id.} at 460–61.
\textsuperscript{31} \textit{Id.} at 460–61 n.4.
\textsuperscript{32} \textit{Id.} at 461 (“Such a container may, of course, be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.”).
II. LOWER COURTS’ ANALYSES OF WARRANTLESS CELL PHONE SEARCHES

Lower courts have come to a variety of conclusions when dealing with searches of cell phones incident to arrest. One of the most prominent cases examining a search of a cell phone as a search incident to arrest is *United States v. Finley*. 33 Police officers conducted a valid traffic stop on the van Finley was driving after observing an informant buy narcotics from a passenger in the vehicle. 34 After searching the van and finding additional drug paraphernalia, officers arrested both Finley and his passenger. 35 Upon searching Finley’s person, officers found a cell phone, but did not search it until they went to his passenger’s residence, where agents were conducting a search pursuant to a prior warrant for the residence. 36 Several text messages found on Finley’s phone implicated him in narcotics trafficking, and after the police confronted Finley with these messages, he admitted to distributing marijuana. 37 Although the Fifth Circuit held that Finley had a reasonable expectation of privacy in his phone and its contents, the court upheld the search. 38 In doing so, the court stated that “[p]olice officers are not constrained to search only for weapons or instruments of escape on the arrestee’s person; they may also, without any additional justification, look for evidence of the arrestee’s crime on his person in order to preserve it for use at trial.” 39 Since the cell phone was found on Finley at the time of his arrest, the court upheld the search, finding that the search was comparable to a search of a closed container. 40 In December 2012, the Fifth Circuit declined to overrule *Finley* in light of recent Supreme Court case law and instead upheld the search of a suspect’s cell phone incident to his arrest for intent to

33. *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007).
34. *Id.* at 253–54.
35. *Id.* at 254.
36. *Id.*
37. *Id.* at 254–55.
38. *Id.* at 259.
39. *Id.* at 259–60.
distribute and possess marijuana, again analogizing a cell phone to a container.41

A year after Finley, in United States v. Young, the Fourth Circuit followed the Fifth Circuit’s lead and upheld the search of a suspect’s cell phone incident to his lawful arrest on the theory of preserving evidence.42 Young’s girlfriend consented to a search of her apartment after informing police of drug activities on its premises.43 Two days later, the police returned and arrested Young and an accomplice.44 Upon searching Young’s person, officers found a cell phone, searched its text messages without a warrant, and wrote down the contents.45 The court found that “officers had no way of knowing whether the text messages would automatically delete themselves or be preserved,” therefore permitting a search to occur incident to arrest.46 In United States v. Murphy, the Fourth Circuit reaffirmed this holding and rejected arguments that the storage capacity of a phone affects whether police may search a phone incident to arrest.47

But not all courts have followed the reasoning of the Fifth Circuit. For instance, the Northern District of California disagreed with Finley, and found a cell phone search to be impermissible as a search incident to arrest. In United States v. Park, defendant Park was arrested after officers observed other defendants leave items at an apartment that Park and an accomplice then entered.48 Pursuant to a search warrant, the officers entered the apartment and observed evidence of marijuana cultivation.49 After being transported to the police station, all defendants were booked and their property, including their cell phones, was placed into envelopes for safekeeping.50 In an attempt to find fellow conspirators,


42. United States v. Young, 278 F. App’x 242, 245–46 (4th Cir. 2008) (per curiam) (“[B]ased upon . . . the Fifth Circuit’s like conclusion, and the manifest need of the officers to preserve evidence, we conclude that the officers permissibly accessed and copied the text messages on the phone during the search incident to arrest” (citing Finley, 477 F.3d at 259–60)).

43. Id. at 244.

44. Id.

45. Id.

46. Id. at 245.

47. United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).


49. Id. at *1–2.

50. Id. at *2.
the officers searched the phones’ address books.\textsuperscript{51} The court concluded that a modern cell phone is similar to a laptop computer rather than the address books and pagers often found on a person incident to arrest, due to the phone’s “capacity for storing immense amounts of private information.”\textsuperscript{52} Since the officers examined the phones long after the initial arrest, the court found that the search of the cell phone was beyond the rationales of ensuring police safety and preserving evidence and was therefore purely investigatory.\textsuperscript{53} The court held that officers were lawfully permitted to seize the cell phones incident to arrest but were required to obtain a warrant in order to search the phones’ contents “due to the quantity and quality of information that can be stored on a cellular phone.”\textsuperscript{54}

In \textit{State v. Smith}, the Ohio Supreme Court agreed with Park’s conclusion that when the search of a cell phone fails to further the twin justifications of officer safety and preservation of evidence, the evidence must be suppressed.\textsuperscript{55} But it disagreed with Park’s rationale that cell phones are similar to laptops, finding that modern cell phones are still phones, and thus distinguishable from laptops.\textsuperscript{56} Smith’s arrest stemmed from the confession of a drug user who claimed Smith was her dealer.\textsuperscript{57} Upon his arrest, officers found and searched Smith’s cell phone to examine the call records and phone numbers to confirm the buyer’s story.\textsuperscript{58} The court specifically held that cell phones are not analogous to closed containers and an officer must obtain a warrant, even when searching incident to arrest, prior to searching a cell phone’s contents.\textsuperscript{59}

At least one court has reasoned that a search incident to arrest, when based on the premise of preserving evidence, must arise from a desire to preserve evidence of the specific crime for which the suspect

\textsuperscript{51} Id. at *3–5. The record is unclear if the search was done prior to booking or after, but it was clear that the search was done at the station—over an hour after the arrest. Id.

\textsuperscript{52} Id. at *8. The court continued to state that “a search of [a laptop is] substantially more intrusive than a search of the contents of a lunchbox or other tangible object.” Id. (quoting United States v. Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006)).

\textsuperscript{53} Id.

\textsuperscript{54} Id. at *9.

\textsuperscript{55} State v. Smith, 920 N.E.2d 949 (Ohio 2009).

\textsuperscript{56} Id. at 955.

\textsuperscript{57} Id. at 950.

\textsuperscript{58} Id.

\textsuperscript{59} Id. at 955.
is being arrested.60 In United States v. Quintana, police arrested Quintana for driving with a suspended license.61 While legally searching the vehicle with Quintana’s consent, the officer smelled marijuana but found no evidence of marijuana in the vehicle.62 Officers then searched Quintana’s phone in order to find evidence to prove his marijuana use.63 After finding a picture of a marijuana grow house on the phone, officers proceeded to the address listed on Quintana’s license, finding further evidence of marijuana cultivation.64 The court stated that since the suspect was arrested for driving with a suspended license the officer was not attempting to preserve evidence of the crime and he was unjustified in his warrantless search of the cell phone.65 The court suppressed the photograph and further evidence found at Quintana’s home.66

The Seventh Circuit, in United States v. Flores-Lopez, upheld the search of a cell phone when the search was conducted solely to find the phone’s number as a valid search incident to arrest.67 Flores-Lopez was arrested after an informant overheard a conversation between him and another dealer that methamphetamines would be delivered to a garage at a particular time.68 After the drugs arrived, officers arrested Flores-Lopez and his associate and proceeded to search both him and the vehicle in which Flores-Lopez had brought the drugs.69 Officers found one cell phone on Flores-Lopez and two more in his truck.70 Subsequently, police officers searched each cell phone to find its telephone number, which the officers then used to subpoena the call history from the provider, including the phone call overheard by the informant.71 The court found that even a negligible risk that evidence on the phone could be wiped validated searches of smart phones, “provided it’s no more invasive than, say, a frisk, or the

61. Id. at 1295.
62. Id.
63. Id. at 1295–96.
64. Id. at 1296.
65. Id. at 1300 (“This type of search is not justified by the twin rationales of Chimel and pushes the search-incident-to arrest doctrine beyond its limits.”).
66. Id. at 1306.
68. Id. at 804.
69. Id.
70. Id.
71. Id.
search of a conventional container, such as Robinson’s cigarette pack, in which heroin was found.\textsuperscript{72} Judge Posner, writing for the court, declined to determine what level of risk would be required to justify a more invasive search since those facts were not before the court.\textsuperscript{73}

As the above cases illustrate, lower courts cannot reach a unanimous conclusion on how to treat cell phone searches incident to arrest. Lower courts have variously permitted police officers to search any cell phone incident to arrest, prohibited police officers from searching any phone without a warrant, or applied a standard in between. As such, police officers struggle to determine which phones they may legally search under the Fourth Amendment. This Comment posits that a workable standard based on Supreme Court precedent already exists.

\section*{III. How \textit{Gant} and \textit{Jones} Affect Smart Phones}

To date, the Supreme Court has never decided a case involving the search of a smart phone, whether incident to arrest or otherwise. In fact, the Court’s examination of developing technologies has been limited to a few cases involving technologies such as wiretapping, aerial photography, heat-sensing technology, and most recently a GPS sensor.\textsuperscript{74} The closest the Supreme Court has come to examining a search of a smart phone was examining the legality of searching an employee’s text messages through a city-owned pager.\textsuperscript{75} The Supreme Court decided that the search of the pager was valid on the exceedingly narrow grounds that the special needs of the workplace justified a warrantless search.\textsuperscript{76} The Court expressly declined to examine whether the defendant’s privacy expectations were implicated by the search or whether any other exceptions to the warrant requirement permitted the search.\textsuperscript{77} But two of the Court’s recent decisions—\textit{Arizona v. Gant}\textsuperscript{78} and \textit{United States v. Jones}\textsuperscript{79}—may shed

\textsuperscript{72} Id. at 809.
\textsuperscript{73} Id. at 810.
\textsuperscript{74} See Daniel T. Pesciotta, Note, \textit{I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century}, 63 Case W. Res. L. Rev. 187 (2012) (examining Supreme Court cases involving both technology and the Fourth Amendment and concluding that the \textit{Katz} reasonable-exception-of-privacy test is still relevant in today’s technologically advanced society).
\textsuperscript{75} City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
\textsuperscript{76} Id. at 2630.
\textsuperscript{77} Id. at 2631.
\textsuperscript{78} Arizona v. Gant, 556 U.S. 332 (2009).
light upon what standard the Court would apply to searches of smart phones incident to a lawful arrest.

A. Does Gant Affect Warrantless Searches Outside Vehicles?

In the 2009 decision Arizona v. Gant, the Supreme Court, per Justice Stevens, held that officers may not search a suspect’s vehicle incident to his arrest when the suspect is handcuffed and secured inside a police car.\(^{80}\) Officers arrested Gant for driving with a suspended license and proceeded to handcuff and lock him in the back of the police car.\(^{81}\) Once Gant was secure, officers searched his vehicle and discovered a bag of cocaine.\(^{82}\) Gant opposed the introduction of the cocaine as evidence at his trial, arguing that the search failed to meet the original justifications for the search incident to arrest doctrine: officer safety and evidence preservation.\(^{83}\) The Court held that

\[
\text{[a] rule that gives police the power to conduct such a search whenever an individual is caught committing a traffic offense, when there is no basis for believing evidence of the offense might be found in the vehicle, creates a serious and recurring threat to the privacy of countless individuals.}^{84}
\]

Although the Court was speaking of the privacy interest owners have in their vehicles, the same argument could be made for the privacy interest in one’s cell phone. The Court’s statement in Gant appears to apply to any situation in which officers attempt to conduct a broad search of a suspect’s person and effects, despite his expectation of privacy, simply because the suspect has been arrested. Unanimously, each court to expressly examine the issue has found that a suspect has a legitimate expectation of privacy in his phone and its contents,\(^{85}\) and the Supreme Court should agree and find an

81. Id. at 336.
82. Id.
83. Id.
84. Id. at 345.
85. See, e.g., United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007) (“In these circumstances, we conclude that Finley had a reasonable expectation of privacy in the call records and text messages on the cell phone.”); United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009) (“An owner of a cell phone generally has a reasonable expectation of privacy in the electronic data stored on the phone.”); United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007) (“[D]ue to the quantity and quality of information that can be stored on a cellular phone, a cellular phone should not be characterized as an element of individual’s clothing or person, but rather as a ‘possession[] within an arrestee’s immediate control [that has] fourth amendment protection at the station house.’” (alteration in
expectation of privacy to which Gant’s holding would apply. Therefore, if the Supreme Court were to agree that there is a reasonable expectation of privacy in a cell phone and its contents, it would find that a rule permitting the search of any cell phone incident to arrest would be a gross invasion of privacy, and thus unconstitutional.

In Gant, the Court explicitly returned to the reasoning put forth in Chimel, stating that searches incident to arrest are limited to the area within the arrestee’s immediate control, meaning the area from which he might obtain a weapon or destroy evidence.86 But the Court found 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.’”87 Although this permission to search based on reasonable belief evidence will be found does not stem from Chimel itself, the Court believed that the lesser privacy interest in the vehicle permitted a search incident to arrest to occur. Similarly, circumstances unique to smart phones permit searches incident to arrest in limited circumstances.88

B. Does Jones Affect Smart Phone Searches?

In United States v. Jones, the Supreme Court reaffirmed the traditional trespass theory of the Fourth Amendment.89 The Court was confronted with the issue of whether evidence must be suppressed when officers placed a GPS tracking device on a suspect’s vehicle in order to observe his movements over a four-week period.90 Although the government had initially obtained a warrant, the officers failed to comply with its requirements, placing the device on the vehicle outside the issuing court’s jurisdiction and outside the timeframe permitted by the court.91 The government conceded the failure to comply and instead argued that no warrant was required in this

86. Gant, 556 U.S. at 339.
87. Id. at 343 (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring) (determining that a vehicle’s reduced expectation of privacy permits a broader search incident to arrest)).
88. See Part IV, infra.
90. Id. at 948.
91. Id.
case. The Court held that the government’s warrantless trespass onto a citizen’s private property is considered a search. Although many recent cases focused solely on whether a suspect had a reasonable expectation of privacy in the item being searched, the Court maintained that the trespass theory and reasonable-expectation-of-privacy theory are not mutually exclusive. Since the government “physically intrud[ed] on a constitutionally protected area” the Court invalidated the search and ordered the evidence suppressed. Every court to address the issue of warrantless searches of cell phones has found a search occurred, but the Jones opinion has stirred debate as to whether officers can use a smart phone’s internal GPS capabilities to track a suspect.

In her concurrence, Justice Sotomayor questioned if the reasonable-expectation-of-privacy test could continue to provide guidance for courts in the wake of new technological advances. Sotomayor stated that “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” In the current digital age, smart phone users disclose the numbers they call, the websites they visit, and the people to whom they send e-mails to their Internet service providers, and even where they bank may be shared. Justice Sotomayor “would not assume that all information

92. Id. at 948 n.1.
93. Id. at 949 (“The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”).
94. Id. at 952 (“[T]he Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”) (emphasis in original); see also id. at 954–55 (Sotomayor, J., concurring) (“[E]ven in the absence of a trespass, ‘a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.’ ” (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001))).
95. Id. at 950 n.3 (majority opinion).
98. Id.
99. See Shane Kite, The Five Best Mobile Banking Apps Now, Am. Banker (October 1, 2010), http://www.americanbanker.com/btn/23_10/the-five-best-mobile-apps-now-1026278-1.html. Not only do people access their bank on their cell phones, they can also pay for purchases and
voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” Under this theory, individuals should not have less of an expectation of privacy in their smart phones simply due to the amount of information that is shared with the cell phone company or other third parties.

IV. WARRANTLESS SMART PHONE SEARCHES ARE PERMISSIBLE IN LIMITED CIRCUMSTANCES

Many commentators have spent countless pages arguing that Chimel should not apply to the search of a cell phone, and the application of Gant to smart phone searches only clarifies that warrantless searches may not be upheld as searches incident to arrest. Gant illustrates the Court’s resolve to return to the initial rationales behind the search incident to arrest doctrine. Jones, especially Sotomayor’s concurrence, explains that without a warrant the government cannot intrude into a constitutionally protected area, and that the current era of technological advances mandates that smart phone users be given Fourth Amendment protection consonant with at least a minimum of an expectation of privacy.


100. Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (“Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.” (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting))).

101. See, e.g., Charles E. MacLean, But, Your Honor, A Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest, 6 Fed. Cts. L. Rev. 37, 38 (2012) (arguing that cell phones are not like cigarette packs, pagers, wallets, or address books simply because they are “likewise small, carried in pockets, and can contain personal information”); see also Eunice Park, Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Occasion-to-Arrest Exception to the Cell Phone as “Hybrid”, 60 Drake L. Rev. 429, 494 (2012) (“[L]aw enforcement officers may search the contents of a cell phone seized incident to a valid custodial arrest if the contents are reasonably likely to yield evidence related to arrest, with a presumption that text messages, e-mail logs, and call logs are searchable. Law enforcement officers may search other reasonably related contents when an exigency exists regarding safety.”). But see Adam M. Gershowitz, Password Protected? Can a Password Save Your Cell Phone From a Search Incident to Arrest?, 96 Iowa L. Rev. 1125, 1174 (2011) (arguing that even a password-protected cell phone may be searched incident to arrest without a warrant).
A. A Cell Phone Is Not a Container

New York v. Belton held that officers are permitted to search containers found within an arrestee’s control.\(^\text{102}\) And several courts have specifically held that cell phones should be considered containers, thereby permitting them to be searched incident to arrest.\(^\text{103}\) On the other hand, several courts have determined that cell phones are not analogous to containers.\(^\text{104}\) This is the better path— due to the vast amounts of data contained in a phone, and the phone’s inability to hold tangible items, courts should find that cell phones are not analogous to ‘containers.’

As noted in State v. Smith, the Supreme Court specifically stated in Belton that the definition of “container” includes only those objects that may hold a physical object within it.\(^\text{105}\) Additionally, the general definition of containers does not encompass cell phones because a cell phone is not “a receptacle . . . for holding goods.”\(^\text{106}\) Cell phones are generally small devices with no space to hold another physical object inside. The containers contemplated by the Supreme Court included such items as a cigarette pack in Robinson\(^\text{107}\) and a jacket in Belton.\(^\text{108}\) A cigarette pack or jacket cannot compare with the sheer amount of data found on today’s smart phones, including bank records and personal documents that police would normally need a warrant to access. Unless the Court expands its legal definition of containers, lower courts should find that cell phones are not analogous to containers.

Additionally, the Court permitted the search of Robinson’s cigarette pack because the officer testified that he could not determine the contents.\(^\text{109}\) Police officers know, however, that smart phones


\(^{103}\) See, e.g., United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (defendant conceded that the cell phone was analogous to a container); People v. Diaz, 244 P.3d 501, 505 (Cal. 2011) (likening a cell phone to Robinson’s cigarette package).


\(^{105}\) Smith, 920 N.E.2d at 954 (“‘Container’ here denotes any object capable of holding another object.” (citing Belton, 453 U.S. at 460 n.4)).


\(^{108}\) Belton, 453 U.S. at 454.

\(^{109}\) Robinson, 414 U.S. at 223.
contain information that is not “intrinsically dangerous.” Since officers know the item likely poses no risk of harm, and the item is not analogous to the Supreme Court’s “container,” officers should not be permitted to search smart phones incident to arrest. This Comment acknowledges that some commentators argue that the data inside the cell phone is analogous to the physical objects held in containers, since it is simply electronic information. But this Comment emphasizes the cases in which courts specifically held that the vast amounts of data on a phone differentiate it from traditional containers. This Comment posits that Gant should control and officers should only be permitted to search a smart phone when they have reasonable suspicion that the smart phone contains evidence of the crime of arrest.

B. Smart Phones Deserve Privacy Equaling Computers

Commentators often compare smart phones to computers and the differences between the two are becoming fewer with each passing year. Most courts addressing the issue have found that computers have a heightened expectation of privacy and require police to obtain a specific warrant for the computer prior to searching its contents. According to courts, “analogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life.”

With each passing year “the line between cell phones and personal computers has grown increasingly blurry.” Today, both smart phones and computers are exceedingly mobile devices. Consumers can


113. Park, supra note 101, at 478; Stewart, supra note 110, at 593; Bryan Andrew Stillwagon, Bringing An End to Warrantless Cell Phone Searches, 42 Ga. L. Rev. 1165, 1201 (2008).

114. See, e.g., United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (holding that search warrants for computers must clearly define the information being sought on the computer).

115. United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011); see also United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (“Relying 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.” (internal quotation marks omitted)).

purchase netbooks\textsuperscript{117} or tablets,\textsuperscript{118} which can fit into a purse or small backpack and contain many of the same capabilities as laptop computers.\textsuperscript{119} Today, laptops can download programming “which includes voice, video, and instant message capabilities” similar to that used in cell phones.\textsuperscript{120} Voice-Over-Internet Protocol was created to replace telephone networks and permits computers to call other computers, or even telephones.\textsuperscript{121} Cloud computing software permits users to access their data through the Internet no matter what technology they are using.\textsuperscript{122} With cloud computing software, a consumer can carry every file from their computer with them on their smart phone. Lastly, although courts seem willing to grant greater protections to computers, a computer could be wiped just as a smart phone may.\textsuperscript{123} Since the differences between smart phones and personal computers are becoming increasingly fewer, courts should recognize that smart phones contain the same expectations of privacy as computers and treat warrantless searches of smart phones in the same manner. Therefore, courts should require reasonable suspicion in the particular parts of the phone being searched.

C. Limited Exigency Created by Remote Wiping

That a smart phone could be remotely deleted does create a minor exigency, but not to the extent that every smart phone can be

\begin{itemize}
  \item\textsuperscript{117} Netbook, \textsc{Encyclopedia Britannica}, http://www.britannica.com/EBchecked/topic/1498289/netbook (last visited Mar. 9, 2013).
  \item\textsuperscript{118} Tablet Computer, \textsc{Encyclopedia Britannica}, http://www.britannica.com/EBchecked/topic/1740658/tablet-computer (last visited Mar. 9, 2013).
  \item\textsuperscript{119} The differences between a tablet computer and a smart phone are continually diminishing, and soon there may be no difference at all. See, \textit{e.g.}, Michael A. Prospero, \textit{Living (Really) Large}, \textsc{Laptop Magazine}, May 2012, at 44 (describing a cell phone, the Samsung Galaxy Note, with the full capabilities of a tablet computer); Kevin C. Tofel, \textit{Asus PadFone 2 is a Modular Phone and Tablet Combo}, \textsc{Gigaom} (Oct. 16, 2012, 12:27 PM), http://gigaom.com/mobile/asus-padfone-2-is-a-modular-phone-and-tablet-combo (describing a tablet powered by a cell phone).
  \item\textsuperscript{120} Skype, \textsc{Encyclopedia Britannica}, http://www.britannica.com/EBchecked/topic/1516582/Skype (last visited Mar. 9, 2013).
  \item\textsuperscript{121} Id.
  \item\textsuperscript{122} Cloud Computing, \textsc{Encyclopedia Britannica}, http://www.britannica.com/EBchecked/topic/1483678/cloud-computing (last visited Mar. 9, 2013); see also Sara J. Kohls, Note, \textit{Searching the Clouds: Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account}, \textsc{4 Case W. Res. J.L. Tech. & Internet} 169 (2012) (describing cloud computing, why people use it, and whether service providers may access those files).
  \item\textsuperscript{123} Remote Delete Laptop Data for Enterprise, \textsc{Druva}, http://www.druva.com/safepoint/remote-delete (last visited Mar. 9, 2013).
\end{itemize}
searched by officers. Although courts have found that the risk of remote wiping permits searching cell phones incident to arrest, the data wiped may still be available for officers to find at a later date. Thus, searching a cell phone incident to arrest is not be required.

Remote wiping “can reset a mobile phone to the factory default condition.” According to law enforcement, an arrestee’s accomplices may be able to wipe the phone prior to officers obtaining a search warrant. “However, no data removal process leaves a mobile device as free from residual data as when it’s new. Recovery of data from a mobile device may still be possible using sophisticated tools.” Although it may be expensive to obtain the sophisticated tools necessary to access the removed data, such tools reduce the exigency created by remote wiping technologies.

Alternatively, officers may prevent a remote wipe from occurring by taking simple steps to protect the phone. For example, most remote wipe technology requires the smart phone to be powered on and officers could simply remove the battery from the device, or power down the phone, as they await a warrant. Additionally, inexpensive devices called Faraday enclosures prevent the remote wipe signal from reaching the phone. Faraday enclosures shield their

124. See United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) (finding that it is “conceivable” for confederates to wipe data from a cell phone before the government could obtain a search warrant); United States v. Salgado, No. 1:09–CR–454–CAP–ECS–5, 2010 WL 3062440, at *4 (N.D. Ga. June 12, 2010) (“At the time the cellular phone came into [police] possession the data on the phone could have been altered, erased, or deleted remotely.”); see also United States v. Young, 278 F. App’x 242, 245–46 (4th Cir. 2008) (per curiam) (finding that officers must search the phone immediately because text messages can be deleted).


126. Ben Grubb, Remote Wiping Thwarts Secret Service, ZDNet (May 18, 2010, 4:43 GMT), http://www.zdnet.com/remote-wiping-thwarts-secret-service-1339303239; see also Park, supra note 101, at 493 (“As consumers, and criminals in particular, become more skillful in their use of smart phones, they will more frequently take advantage of the remote wipe or automatic deletion feature to banish incriminating data from their phones.”).


128. See Grubb, supra note 126; see also Flores-Lopez, 670 F.3d at 808 (“Without power a cell phone won’t be connected to the phone network and so remote wiping will be impossible.”).

129. MacLean, supra note 101, at 50.
contents from electromagnetic radiation and effectively prevent cell phone signals from reaching a phone held inside, therefore eliminating the risk of losing evidence.\textsuperscript{130}

In today’s digital age, the information stored on a smart phone is often stored in multiple places, and wiping the phone would not destroy the actual data sought by officers.\textsuperscript{131} Smart phones include contacts, calendars, email accounts, and more,\textsuperscript{132} and such information is often stored on servers and not solely on the phone.\textsuperscript{133} If the officers are unable to prevent the smart phone’s contents from being wiped, they may seek a warrant to search the servers just as they may have done for the phone itself. In fact, the Supreme Court has already held that there is no expectation of privacy in the numbers called,\textsuperscript{134} and therefore officers could quickly subpoena the phone company requesting the call logs from the phone.

Although remote wipe technology does create a risk that evidence may be deleted, the data itself may still be accessible at a later time. Since the data may still be accessible, courts should not find that searches incident to arrest are required due to the risks posed in waiting for a warrant.

D. Setting a Standard

The standard set out in \textit{Gant} for searches of motor vehicles incident to arrest\textsuperscript{135} should be applied to smart phones as well. Consumers possess a reasonable expectation of privacy in their phones and, without an exception to the warrant requirement, any evidence

\textsuperscript{130} Id.

\textsuperscript{131} See Thomas Porter, \textit{The Fallacy of Remote Wiping}, ZDNET (July 12, 2012, 1:55 PM, GMT), http://www.zdnet.com/the-fallacy-of-remote-wiping-7000000611 (“‘You nuked my entire device?’ That’s OK. I replicated all of the important stuff to Facebook, several different cloud storage providers and my home computer using Google +, Evernote, Pocket, Delicious, Direct USB, etc.”).


\textsuperscript{133} \textit{Cloud Computing}, supra note 122. One example of such storage is Apple’s cloud storage, “iCloud.” \textit{See also iCloud}, APPLE, http://www.apple.com/icloud (last visited Mar. 9, 2013) (“iCloud does more than store your content—it lets you access your music, photos, calendars, contacts, documents, and more, from whatever device you’re on.”).

\textsuperscript{134} Smith v. Maryland, 442 U.S. 735, 745 (1979).

\textsuperscript{135} Arizona v. Gant, 556 U.S. 332, 335 (2009) (holding that “a vehicle search incident to a recent occupant’s arrest after the arrestee has been secured and cannot access the interior of the vehicle” is not authorized, but that “circumstances unique to the automobile context justify a search incident to arrest when it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle”).
seized must be suppressed. “While no particularized suspicion is required for a search incident to arrest, there must be, at a minimum, the possibility of destruction of evidence or a threat to an officer’s safety.” But due to the vast amounts of data found on smart phones, officers should be required to limit their searches to those areas of the phone that might contain relevant evidence.

At least one commentator has argued that officers are sometimes searching for the telephone numbers of co-conspirators, which may change prior to the officers being able to obtain a warrant. In this type of situation, however, would permit a search of the phone’s contacts since it is reasonable to assume that evidence would be found on the phone. This Comment need not set a specific standard for this type of exigency because the standard would already permit a valid search to occur.

Conclusion

Although courts have been left to analyze warrantless smart phone searches incident to arrest without guidance from the Supreme Court, recent cases clarify the standard that should be applied. Following the Court’s decision in , courts should return to the twin justifications from . In order to permit a search incident to arrest of a defendant’s smart phone, police should determine if it was reasonable to believe evidence related to the arrest would be found on the phone prior to the search. Although officers will not be permitted to search smart phones incident to every arrest, the specific circumstances surrounding an arrest may implicate the reasonable belief necessary to permit a search. In the hypothetical discussed in the Introduction to this Comment, officers were not aware of any co-conspirators working with White, so it would be unreasonable to search his phone and the

136. Stewart, supra note 110, at 593 (citing Chimel v. California, 395 U.S. 752, 763 (1969)).

137. This standard would be similar to that required in searches of computers, even pursuant to a warrant. See United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (requiring officers to sort the various documents found on a computer and if the officer comes across intermingled documents, the officer should request a new warrant covering the new documents).

138. See Daniel K. Gelb, US v. Flores-Lopez: Does the Phone Booth Now Reside Inside the Phone?, 36 CHAMPION 18, 19 (May 2012) (explaining that co-conspirators may replace their SIM cards each day, therefore obtaining new phone numbers each time, which creates an exigency to obtain phone numbers before they change).

139. , 556 U.S. 332.

140. Chimel, 395 U.S. 752.
evidence must be suppressed. Even if officers held a reasonable suspicion that White’s phone contained contact information for his co-conspirators, the search would be limited to the phone’s contact list and recent calls—searching the phone’s photographs would be impermissible.

Sara M. Corradi†

† J.D. Candidate, 2013, Case Western Reserve University School of Law; B.A., summa cum laude, 2009, Southern Methodist University. A special thank you goes to Sara Kohls for reading a prior draft and giving her invaluable advice and to my friends and family for their support.