Florida State University Law Review

Volume 39 | Issue 4 Article 5

2012

The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right to Be Free Fom Unreasonable Searches and Seizures

Mina Ford
0@0.com

FLORIDA STATE UNIVERSITY
LAW REVIEW

THE WHOLE WORLD CONTAINED: HOW THE UBIQUITOUS USE OF MOBILE PHONES UNDERMINES YOUR RIGHT TO BE FREE FROM UNREASONABLE SEARCHES AND SEIZURES

Mina Ford

VOLUME 39 SUMMER 2012 NUMBER 4

Recommended citation: Mina Ford, *The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right to Be Free From Unreasonable Searches and Seizures*, 39 FLA. ST. U. L. REV. 1077 (2012).

THE WHOLE WORLD CONTAINED: HOW THE UBIQUITOUS USE OF MOBILE PHONES UNDERMINES YOUR RIGHT TO BE FREE FROM UNREASONABLE SEARCHES AND SEIZURES

MINA FORD*

I. FOUNDATIONS 1081
  A. *The Automobile Exception* 1082
  B. *Search Incident to Arrest* 1083
  C. *Closed Containers* 1085
II. TECHNOLOGY MOVES TOO FAST FOR RIGID RULES 1087
  A. *The Court's Lack of Foresight in* Olmstead 1088
  B. *The Court's Lack of Foresight in* Kyllo 1090
III. CAN COURTS CRAFT A SOLUTION? 1092
  A. *Conflicting Decisions Among State Courts and Courts of Appeals* 1092
    1. Finley *and* Park*: The Early Cases* 1093
    2. *Courts Begin to Fall in Line Behind* Finley 1094
    3. *Flipping the Script on* Finley 1095
      (i) *A Mobile Phone is Not a Container* 1096
      (ii) *An Inventory Search is Not an Investigation* 1096
      (iii) *Searching Data on a Mobile Phone Incident to Arrest Does Not Further the Supreme Court's Justifications for the Search Incident to Arrest Doctrine* 1097
      (iv) *The Exigent Circumstances Rationale for Warrantless Pager-searches Incident to Arrest Should Not Extend to Mobile Phones* 1098
    4. *Bound by Precedent?* 1099
  B. *Some Proposed Solutions* 1100
IV. MOBILE PHONE: MORE THAN A LAPTOP 1102

"I want the world. I want the whole world. I want to lock it all up in my pocket. . . . Give it to me NOW!"[1]

Admit it: you and your mobile phone[2] are virtually inseparable. You regularly send and receive e-mail from the device. You and your mobile phone are in constant contact.[3] As Americans become

---

* J.D., cum laude, Florida State University College of Law, 2012; B.A., English, Florida State University, 2002. I am grateful to Professor Wayne Logan for sparking and encouraging my fascination with criminal procedure.

1. These are the famous words of fictional spoiled brat, Veruca Salt, as delivered musically in Willy Wonka & the Chocolate Factory. Ms. Salt, of course, was not speaking of her desire for constant access to the Internet, but rather her desire for a golden goose. WILLY WONKA & THE CHOCOLATE FACTORY.

2. Throughout this Note, I will use the term "mobile phone" to refer to a wireless telephone one typically carries in her pocket or purse. This term is interchangeable with the term "cell phone" or "cellular phone."

3. The chance that I am accurately describing you is quite high. "Eight in ten American adults . . . own a [mobile] phone of some kind." AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, AMERICANS AND THEIR CELL PHONES 5 (Aug. 15, 2011) [hereinafter SMITH, CELL PHONES], http://pewinternet.org/~/media//Files/Reports/2011/cell%20Phones%202011.pdf. In April 2009, the Pew Internet & American Life Project found that 25% of mobile phone

increasingly tethered to their mobile phones, privacy considerations become apparent. In our fervor to have the fastest, the best, the most connected mobile phone, we have lost sight of some of the negative consequences of being hyper-connected. As users demand and manufacturers provide quicker access to e-mail, the Internet, and data, mobile phones become a repository for vast quantities of information. This information is highly concentrated and easily accessible from the mobile device. As this occurs, Fourth Amendment concerns are necessarily implicated because more and more material becomes vulnerable to discovery by law enforcement officers during a search. The United States Supreme Court has developed a Fourth Amendment jurisprudence that, carried to its logical conclusion, threatens to open up an immeasurable amount of private and personal information to agents of the government.[4]

In the Fourth Amendment inquiry into the reasonableness of a search, mobile phones—and "smartphones" with Internet capabilities in particular[5]—should be afforded the same level of protection that laptop computers are afforded. At present, case law is sparse regarding searches of computers when those computers are discovered inside a vehicle or otherwise outside the home;[6] however, mobile phones arguably should be treated as if they were computers, as the distinction has become blurred and is likely to become more blurred in the future.[7] Given that many mobile phones now provide instant access to the user's e-mail and other Internet

---

users accessed the Internet wirelessly via mobile phone; that number jumped to 38% by May 2010 and 44% by May 2011. *See* AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, MOBILE ACCESS 2010 at 12 (July 7, 2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Mobile_Access_2010.pdf; *see also* SMITH CELL PHONES, *supra*, at 5-6.

4. For a somewhat recent analysis of these issues from a law enforcement perspective, see Carl Milazzo, *Chief's Counsel, Searching Cell Phones Incident to Arrest: 2009 Update*, POLICE CHIEF, *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&issue_id=52009&category_ID=3.

5. Mobile phones possessing these capabilities are often referred to as "smartphones." *See* Jo Best, *Analysis: What is a Smart Phone?*, ZDNET.CO.UK (Feb. 13, 2006, 1:05 PM), http://www.zdnet.co.uk/news/mobile-it/2006/02/03/analysis-what-is-a-smart-phone-40148352/. PC Magazine Encyclopedia defines a smartphone as "[a] cellular telephone with built-in applications and Internet access." *Definition of: Smartphone*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp (last visited July 1, 2012). One recent study has shown that 82% of smartphone users check and receive e-mail through their devices. GOOGLE/IPSOS OTX MEDIACT, THE MOBILE MOVEMENT: UNDERSTANDING SMARTPHONE USERS 11 (Apr. 2011), http://www.gstatic.com/ads/research/en/2011_TheMobileMovement.pdf. For additional information regarding the smartphone habits of Americans, see AARON SMITH, SMARTPHONE ADOPTION AND USAGE, PEW INTERNET & AM. LIFE PROJECT (July 11, 2011), http://pewinternet.org/Reports/2011/Smartphones/Summary.aspx.

6. There is, however, an increasingly large body of case law dealing with searches of mobile phones under these circumstances. *See infra* Part III.A.

7. United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. 2007) ("[T]he line between cell phones and personal computers has grown increasingly blurry . . . .").

communications,[8] any doctrine that treats a mobile phone like an ordinary closed container[9] in Fourth Amendment analysis fails to address meaningful differences in the type and quantity of personal information that is now accessible through a mobile phone and fails to adequately consider privacy concerns of mobile phone users.

The reasonableness clause of the Fourth Amendment of the United States Constitution safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[10] While "houses, papers, and effects" might have been, at ratification, a satisfactory battery of items expressly afforded Fourth Amendment protections, ever advancing technologies have complicated and continue to complicate the judiciary's application of those words to real-life situations.

Since the early years of the United States' sovereignty, Americans have strongly supported the notion that a person enjoys a special sort of privacy in his own dwelling, as evidenced by the writings of John Adams.[11] Both in English common law and in nineteenth-century America, victims of eavesdropping had an actionable nuisance claim against the person who listened in on them surreptitiously.[12] As time and technology have progressed, these protections have expanded and have shaped the country's definition of what type of intercepted communication constitutes a "search" for purposes of the Fourth Amendment. One constant in the Supreme Court's jurisprudence has been its willingness to distinguish addressing information, which is used to convey a communication, from the actual content of a communication. Under this formulation, the collection of addressing information such as telephone numbers does not constitute a search and therefore does not enjoy the Fourth Amendment protection that the content of a telephone call does.[13] Even in the late nineteenth century, the Supreme Court recognized the Fourth Amendment concerns in the contents of a private communication when the Court held that mail could not be intercepted, opened, and read by agents of

8. *See* SMITH, *supra* note 5.

9. The United States Supreme Court has defined a container as "any object capable of holding another object," and has stated that this classification "includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like." New York v. Belton, 453 U.S. 454, 460 n.4 (1981).

10. U.S. CONST. amend. IV.

11. 1 LEGAL PAPERS OF JOHN ADAMS 137 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (describing a man's dwelling house as his "[c]astle").

12. *See* Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 95 (2008).

13. *See* Smith v. Maryland, 442 U.S. 735, 741-42 (1979).

the government absent a warrant.[14] The Court has subsequently upheld the sanctity granted to content information as opposed to addressing information,[15] and this distinction ensures that the court views differently materials that a person affirmatively exposes to the public and materials that a person elects to keep private.[16] Thus, when the government gathers information that the sender has necessarily exposed to others, no "search" has been performed[17] and Fourth Amendment protections do not apply;[18] however, when the government gathers information that a citizen sought to retain as private, the Fourth Amendment is implicated and such information is protected from public exposure.[19]

In this Note, I examine the Supreme Court's Fourth Amendment jurisprudence as it relates to the warrant exceptions approved in searches incident to arrest and searches of automobiles I then analyze the implications these doctrines have for the constitutionality of searches of mobile phones. In Part I, I lay a foundation for further discussion by tracing the history of Fourth Amendment searches of containers in the context of searches incident to arrest made outside the home and searches conducted pursuant to the judicially crafted "automobile exception." In Part II, I explore how the court has handled (and mishandled) other emerging technologies. In Part III, I examine how courts, academics, and legislatures have addressed government searches of mobile phones, and I discuss and critique several scholars' proposals for how the Supreme Court should ultimately handle the issue of increased law enforcement access to private communications via smartphones. Finally, in Part IV, I conclude that in a search a mobile phone should be treated exactly as a laptop is treated and I offer closing remarks with regard to how courts should handle these difficult questions.

---

14. *Ex Parte* Jackson, 96 U.S. 727, 733 (1877). *See also* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (citing *Ex Parte* Jackson affirming the government's need for a warrant prior to opening a wrapped package).

15. United States v. Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008) (discussing Katz v. United States, 389 U.S. 347 (1967) and *Smith*, 442 U.S. 735, and extending the Court's line of reasoning in those cases to e-mail communications). *See also* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.2(a) (3d ed. 2007) (noting that mail, such as a postcard, which does not conceal its contents from the public does not enjoy Fourth Amendment protection). For an enlightening and thorough discussion of the outside/inside and content/non-content dichotomies as they relate to Fourth Amendment jurisprudence in an Internet age, see Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010).

16. *See Katz*, 389 U.S. at 351-52; *Forrester*, 512 F.3d at 511.

17. *Smith*, 442 U.S. at 745-46.

18. *Katz*, 389 U.S. at 351.

19. *Id*. at 351-52.

I. FOUNDATIONS

In the beginning, there was the Fourth Amendment.[20] Of course, its proscription on unreasonable searches and seizures was developed in a context quite different from the one in which today's courts must decide cases. To ponder how the Framers may have felt about a computer or mobile phone search would be an exercise in absurdity. At the time the Fourth Amendment was drafted, the prevailing concern was to provide protection from the issuance of general warrants, upon which the government was entitled to search everything and everywhere without consideration of the purpose or scope of the search.[21] The Fourth Amendment, as is evidenced from its text, requires that a search be reasonable and that a search be conducted only after the issuance of a warrant. Over time, the Court has established various exceptions to the warrant requirement.[22] Generally, however, the reasonableness clause must be satisfied, even where a valid warrant exception applies.[23] For the purposes of

---

20. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

21. Chimel v. California, 395 U.S. 752, 761 (1969) ("The Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence.").

22. Although the Court has described these exceptions as few and as "jealously and carefully drawn," Jones v. United States, 357 U.S. 493, 499 (1958), their proliferation over the years has exploded. Some examples of exceptions to the warrant requirement that the United States Supreme Court has recognized are as follows: *Brigham City*, *Utah v. Stuart*, 547 U.S. 398 (2006) (exigent circumstances); *Griffin v. Wisconsin*, 483 U.S. 868, 87) (special needs); *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973) (consent); *Coolidge v. New Hampshire*, 403 U.S. 443 (1971) (automobile exception); *Chimel*, 395 U.S. 752 (warrantless search incident to arrest). *See also* Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473-74 (1985) (citing more than twenty exceptions to either the probable cause requirement or the warrant requirement of the Fourth Amendment).

23. STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY 32 (9th ed. 2010) ("When an exception to the warrant requirement is applicable, only the reasonableness requirement must be satisfied."). I am of the mind that where the warrant requirement has been dispensed with by one of the Court's judicially crafted warrant exceptions, reasonableness must not be automatically assumed but must be evaluated by the Court. Nevertheless, at least one court facing a mobile phone search issue described the search as falling under an exception to the reasonableness clause, rather than the warrant clause. *See* United States v. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009) ("I see no principled basis for distinguishing a warrantless search of a cell phone from the search of other types of personal containers found on a defendant's person that fall within the *Edwards-Lafayette* exceptions to the Fourth Amendment's reasonableness requirements."). This statement seems, on its face, to be flatly incorrect; in both *Edwards* and *Lafayette*, the Court applied the inventory exception to the warrant requirement and then went on to explain why each of these searches was indeed reasonable as required by the Fourth Amendment. *See* United States v. Edwards, 415 U.S. 800, 802-03, 806 (1974) (applying inventory exception and pointing out that law enforcement officers' actions in seizing evidence was reasonable); Illinois v. Lafayette, 462 U.S. 640, 648 (1983) (applying inventory exception and holding that "it is

this Note, I will briefly describe two of the warrant exceptions: (1) the automobile exception and (2) the search-incident-to-arrest exception.

A. The Automobile Exception

The automobile exception has its roots in *Carroll v. United States*,[24] in which the Supreme Court validated a warrantless search of a vehicle that uncovered "intoxicating liquor" that was being transported illegally.[25] Distilled to its essence, the automobile exception allows law enforcement officers to conduct a warrantless search of a vehicle when there is probable cause to believe that the vehicle contains contraband or evidence of a crime.[26] As the Court has sought to develop and flesh out this exception, it has relied primarily on two justifications: (1) the inherent mobility of automobiles and (2) a decreased expectation of privacy in the contents of an automobile.[27]

In *United States v. Ross*, the Court held that when officers are conducting a warrantless search of a vehicle pursuant to the automobile exception, such officers may look inside closed containers they discover within the vehicle.[28] However, as is often the case, the Court's clear-cut rule was not quite clear enough. In 1982, at the time *Ross* was decided, the Court still had some perplexing precedent to wrestle with. In the late 1970s, the Court held in *United States v. Chadwick*[29] and *Arkansas v. Sanders*[30] that a warrant was required for law enforcement officers to conduct a search of certain containers located inside a vehicle. In *Chadwick*, the Court stated the question as "whether a search warrant is required before federal agents may open a locked footlocker which they have lawfully seized at the time

---

not 'unreasonable' for police, as part of the routine procedure incident to incarcerating an arrested person, to search any container or article in his possession, in accordance with established inventory procedures.").

24. 267 U.S. 132 (1925). It is not entirely certain the Justices handing down that decision knew they were creating a vast blanket exception to the warrant requirement. Nothing in the *Carroll* opinion describes the search that took place as an "exception." *See* Carroll, 267 U.S. at 132-162. In fact, the United States Supreme Court did not use the term "automobile exception" until almost fifty years after the *Carroll* decision. *See Coolidge*, 403 U.S. at 462.

25. *Carroll*, 267 U.S. at 162.

26. *Id*. at 149 ("On reason and authority the true rule is that if the search and seizure without a warrant are made upon probable cause, that is, upon a belief, reasonably arising out of circumstances known to the seizing officer, that an automobile or other vehicle contains that which by law is subject to seizure and destruction, the search and seizure are valid.").

27. United States v. Ross, 456 U.S. 798, 829-31 (1982) (Marshall, J., dissenting) (discussing the historical rationales for the automobile exception to the warrant requirement).

28. *Id*. at 821 ("When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between . . . glove compartments, upholstered seats, trunks, and wrapped packages . . . must give way to the interest in the prompt and efficient completion of the task at hand.").

29. 433 U.S. 1 (1977).

30. 442 U.S. 753 (1979).

of the arrest of its owners, when there is probable cause to believe the footlocker contains contraband."[31] The Court held that a warrant was required under these circumstances.[32] Two years later, the Court seemingly reinforced its *Chadwick* reasoning holding that, absent exigent circumstances, a warrant was required for law enforcement officers to conduct a search of a piece of luggage seized from inside an automobile.[33] The *Ross* Court distinguished *Chadwick* and *Sanders*, pointing out that officers had probable cause to search the luggage at issue in those cases, but did not have probable cause to search the vehicle generally, as was the case in *Ross*.[34]

In *California v. Acevedo*, the Court clarified its interpretation and application of the automobile exception in an apparent attempt to settle any remaining confusion.[35] The Court returned to the case in which the automobile exception was first conceived and interpreted "*Carroll* as providing one rule to govern all automobile searches. The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained."[36] After *Acevedo*, it seems clear that where probable cause exists to believe contraband or evidence is contained within a vehicle, law enforcement officers are empowered to look inside any containers inside the vehicle.

B. Search Incident to Arrest

The Court also recognizes an exception to the warrant requirement in which officers are permitted to conduct a warrantless search of an "arrestee's person and the area 'within his immediate control' " at the time of arrest.[37] Warrantless searches incident to arrest have been justified by the Court on the basis of officer safety.[38] In *Belton*, the Court made clear that *Chimel*'s permissible search of the arrestee's person and the "grab area" around him extended to searches incident to arrest in the automobile context.[39] In the most

31. *Chadwick*, 433 U.S. at 3.

32. *Id*. at 15-16.

33. *Sanders*, 442 U.S. at 766 ("Where . . . the police, without endangering themselves or risking loss of the evidence, lawfully have detained one suspected of criminal activity and secured his suitcase, they should delay the search thereof until after judicial approval has been obtained.").

34. *See* United States v. Ross, 456 U.S. 798, 817 (1982).

35. California v. Acevedo, 500 U.S. 565, 580 (1991). The Court noted that the *Chadwick-Sanders* rule and the holding in *Ross* had caused tremendous confusion among legal scholars, courts, and law enforcement officers. *See id*. at 576-77.

36. *Id*. at 580.

37. Chimel v. California, 395 U.S. 752, 763 (1969).

38. *Id*. (noting the arrestee's ability to reach out and grab "a weapon or destructible evidence").

39. New York v. Belton, 453 U.S. 454, 460 (1981) ("[W]e hold that when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that

recent Supreme Court case to speak on this issue, *Arizona v. Gant*, the Court held that a warrantless search incident to arrest of an automobile occupant is permissible only where the search is confined to a search for evidence related to the arresting offense or in cases where the arrestee is not secured and could conceivably reach the interior of the vehicle.[40]

The Court created an additional wrinkle to the search incident to arrest analysis in 1973 when it announced a search inside a crumpled cigarette package on the person of an arrestee is "not only an exception to the warrant requirement of the Fourth Amendment, but also a 'reasonable' search under that Amendment."[41] Officers arrested Willie Robinson, Jr., for driving with a revoked license,[42] and in the course of their search of Robinson's person they discovered heroin concealed inside a cigarette package inside his coat pocket.[43] The *Robinson* court acknowledged the "unqualified authority of the arresting authority to search the person of the arrestee,"[44] and noted that the validity of a search of the area within an arrestee's control "has been subject to differing interpretations as to the extent of the area which may be searched."[45]

Several state and federal courts have relied on this distinction in *Robinson* to validate as "searches of the person" searches of mobile phones in the pockets of citizens at the time of their arrests.[46] Other courts refuse to classify a mobile phone in an arrestee's pocket as subject to a search-of-the-person analysis, instead ruling that a mobile phone found on the arrestee's person may not automatically be searched as part of a person-search incident to arrest.[47] The traditional basis for the warrantless search incident to arrest has been that it is reasonable for officers to search for "weapons, instruments of escape, and evidence of crime when a person is taken

---

automobile. It follows from this conclusion that the police may also examine the contents of any containers found within the passenger compartment, for if the passenger compartment is within reach of the arrestee, so also will containers in it be within his reach.") (internal citations omitted).

40. 556 U.S. 332, 335 (2009) ("[W]e hold that Belton does not authorize a vehicle search incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle. . . . [W]e also conclude 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.").

41. United States v. Robinson, 414 U.S. 218, 235 (1973).

42. *See id.* at 220.

43. *Id.* at 223.

44. *Id.* at 225.

45. *Id.* at 224.

46. *See infra* Part III.A.

47. *See, e.g.*, United States v. Park, No. CR 05-375 SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007).

into official custody and lawfully detained."[48] This rationale is echoed in *Gant*'s holding that searches incident to arrest must be limited where the suspect has been secured and where there is no reason to believe evidence of crime is contained inside the arrestee's vehicle.[49] Depending on the facts of an arrest and how the Court chooses to interpret the intersection of these related doctrines, a warrantless search of a mobile phone incident to arrest may or may not be deemed reasonable by the Court. For example, in *Edwards*, a search of the arrestee's clothing certainly seemed reasonable, given that the clothes were likely to contain evidence of his crime.[50] However, because officers are empowered to arrest citizens even for extremely minor crimes,[51] it is plausible officers might arrest simply because it gives license to a person-search.

C. Closed Containers

Intermingled in the Court's precedent surrounding warrantless searches of vehicles is the question of whether or not officers may conduct a warrantless search of a container discovered within a vehicle, on the person of an arrestee, or within the arrestee's immediate control. Generally, where an officer meets the requirements of either the search-incident-to-arrest doctrine[52] or conducts a search pursuant to the automobile exception, the court has permitted a search of all containers inside the passenger compartment of the vehicle.[53] The Court has refused to draw a line between types of containers that are more protected than others.[54] If a container is within the arrestee's reach or if officers have probable

48. United States v. Edwards, 415 U.S. 800, 802-03 (1974) (citing *Robinson*, 414 U.S. at 235). *See also id.* at 806 ("When it became apparent that the articles of clothing were evidence of the crime for which Edwards was being held, the police were entitled to take, examine, and preserve them for use as evidence, just as they are normally permitted to seize evidence of crime when it is lawfully encountered.").

49. Arizona v. Gant, 556 U.S. 332, 343 (2009).

50. *Edwards*, 415 U.S. at 806.

51. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 324, 354 (2001) (approving of arrest for failure to wear a seatbelt). "If an officer has probable cause to believe that an individual has committed even a very minor criminal offense in his presence, he may, without violating the Fourth Amendment, arrest the offender." *Id.* at 354.

52. This search authority is limited by Gant to situations in which the arrestee is unsecured or when it is reasonable to believe evidence related to the arresting offense may be found inside the vehicle. *Gant*, 556 U.S. at 343.

53. *See id.*; United States v. Ross, 456 U.S. 798, 800 (1982).

54. *Ross*, 456 U.S. at 822 (noting that the Court refuses to classify some containers as "worthy" and others as "unworthy"). "[A] traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim[s] an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case." *Id.*

cause to believe it contains evidence of the crime of arrest, officers may search without first obtaining a warrant.[55]

But what exactly *is* a "container"? The Supreme Court, in *Belton*, stated that the term "container . . . denotes any object capable of holding another object."[56] Thus, the Court stated, it "includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like."[57]

Is a mobile phone a closed container? Is a laptop a closed container? Does it matter?[58] The closed container analysis is necessarily based on containers that are physical objects capable of holding other physical objects. One need only closely examine the Court's language in *Belton* to confirm this.[59] Given that several state courts and Courts of Appeals have extended the closed container analysis to treat mobile phones as if they were ordinary "objects capable of holding another object,"[60] the Supreme Court is in a position and has a responsibility to outline the contours of this important aspect of Fourth Amendment law.[61] But are the Justices of the Supreme Court equipped to handle this task or could there be a legislative answer?[62]

---

55. *Id*. at 824 ("The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.").

56. New York v. Belton, 453 U.S. 454, 460 n.4 (1981).

57. *Id*.

58. At least one court has rejected the notion that a mobile phone's status as a container is dispositive of the issue. *See* Smallwood v. State, 61 So. 3d 448, 460 (Fla. 1st DCA 2011) ("[W]hether or not a cell phone is properly characterized as a traditional 'container' is irrelevant to whether or not it is searchable upon arrest.").

59. The Belton Court defined a container as "any object capable of holding another object." *Belton*, 453 U.S. at 460 n.4. In 1981, when Belton was decided, the first dictionary definition for the word "object" was "something that is put or may be regarded as put in the way of some of the senses: a discrete visible or tangible thing <saw an ~ in the distance>." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE, UNABRIDGED 1555 (Philip Babcock Gove ed., 1981).

60. *See infra* Part III.A.

61. The Court has had the opportunity to address these issues in the following cases, for which it has denied certiorari: *United States v. Murphy*, 552 F.3d 405 (4th Cir. 2009); *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007); *People v. Diaz*, 244 P.3d 501 (Cal. 2011), *cert. denied*, 132 S.Ct. 94 (2011); *State v. Boyd*, 992 A.2d 1071 (Conn. 2010), *cert. denied*, 131 S.Ct. 1474 (2011); *State v. Smith*, 920 N.E.2d 949 (Ohio 2009).

62. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807-08 (2004) (arguing legislatures are better equipped to adapt to changing technologies and advocating for judicial deference and acquiescence to legislatures until technologies "stabilize"); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1535-36 (2010)

II. TECHNOLOGY MOVES TOO FAST FOR RIGID RULES

"If I'm applying the First Amendment, I have to apply it to a world where there's an Internet, and there's Facebook, and there are movies like . . . 'The Social Network,' which I couldn't even understand."[63]

It is not entirely clear that citizens of the United States can trust the United States Supreme Court to satisfactorily protect our digital privacy. The Court's recent foray into applying constitutional principles to communications devices revealed a startling lack of comprehension regarding a technology that was arguably obsolete by the time the Court ruled.[64] Although the Court's general lack of technological savvy is troubling, more troubling is the Court's apparent inability to appreciate the speed with which new technologies emerge and the potentially negative privacy implications of the Court's holdings as these innovations become widely available to the public.[65] In the earliest era of Fourth Amendment jurisprudence, the speed with which technologies became ubiquitous was quite slow,[66] so the Court did not need to wrestle with rapidly changing technologies. For purposes of demonstrating the Court's unsatisfactory attempts to apply historical principles to new innovations, I will examine two cases where the

---

(discussing a preference for allowing courts to handle regulation of government information-gathering via application and interpretation of the Fourth Amendment).

63. Erik Schelzig, *Supreme Court Justices Must Adapt to Facebook World, Says Breyer*, MSNBC.COM (Nov. 16, 2010 8:14:28 PM), http://www.msnbc.msn.com/id/40224302/ns/technology_and_science-tech_and_gadgets/t/supreme-court-justices-must-adapt-facebook-world-says-breyer/#.TuOWY3r1tdh (quoting Justice Stephen Breyer of the United States Supreme Court).

64. During oral arguments for *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), the Justices fumbled through a series of questions related to text messages sent via pager. Transcript of Oral Argument, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf [hereinafter *Quon* Transcript]. During the questioning, Chief Justice Roberts and Justice Scalia both appeared to be oblivious to the fact that communications sent via pager are transmitted through a third party and do not simply travel directly from one device to another, a consideration integral to understanding the third-party doctrine as it applies to private communications. *See id. at* 49-50. I do not address the third party doctrine in this Note. For two conflicting viewpoints regarding the doctrine, compare Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) with Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009). Similarly, Chief Justice Roberts and Justice Kennedy asked questions suggesting that they did not grasp that a pager is capable of receiving a message at the same time the user is composing a message. *See Quon* Transcript at 44.

65. *See infra* Part II.B.

66. *See* Nicholas Felton, *Consumption Spreads Faster Today*, N.Y. TIMES (Feb. 10, 2008), http://www.nytimes.com/imagepages/2008/02/10/opinion/10op.graphic.ready.html. *See also* Karl Hartig, *Tuning In: Communications Technologies Historically Have Had Broad Appeal for Consumers*, WALL ST. J. CLASSROOM EDITION (1998), *available at* http://www.karlhartig.com/chart/techhouse.pdf.

Court has struggled to craft a rule based on fast-moving technology: *Olmstead v. United States*[67] and *Kyllo v. United States*.[68]

A. The Court's Lack of Foresight in Olmstead

The world's first telephone was patented by Alexander Graham Bell in 1876.[69] By 1910, seven million telephones were in use in the United States.[70] In 1928, the United States Supreme Court granted certiorari in a case that required the Justices to determine whether the Fourth Amendment provided any protection for private communications conducted via telephone.[71] In 1928, at the time the Court ruled in *Olmstead*, approximately 40 percent of American households owned a telephone.[72] In an opinion that perhaps many might find shocking today, the Court held that because telephone wires extend outside the physical exterior of a home, communications conducted on these lines do not enjoy the same Fourth Amendment protections as the inside of a home.[73] The Court based its holding in *Olmstead* on the physical nature of the telephone wires and the fact that the communications intercepted were intended by the sender to extend out into the world for interception or listening in by anyone. The Court stated:

> The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.[74]

Justice Brandeis wrote an elegant and prophetic dissent in which he questioned the effect the majority's holding might have on private

---

67. 277 U.S. 438 (1928) (dealing with telephonic communications), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

68. 533 U.S. 27 (2001) (dealing with thermal imaging technology).

69. *See* PBS, *Technology Timeline: 1750-1990*, PBS.ORG, http://www.pbs.org/wgbh/amex/telephone/timeline/f_timeline.html (last visited July 1, 2012). By 1910, seven million telephones were in use in the United States. HERBERT NEWTON CASSON, THE HISTORY OF THE TELEPHONE at v (1911), *available at* http://books.google.com/ (search "the history of the telephone" and select the first link).

70. CASSON, *supra* note 69. In this book, Casson states, "it is now an indispensible help to whoever would live the convenient life." *Id.* This excited language regarding the ubiquity of the telephone may sound familiar to us today when we think about how dependent we are on the instant availability of e-mail, business documents, and other files on our mobile phones.

71. *Olmstead*, 277 U.S. at 439.

72. Gene Smiley, Economic History Services, *The U.S. Economy in the 1920s*, EH.NET ENCYCLOPEDIA (Feb. 1, 2010), http://eh.net/encyclopedia/article/smiley.1920s.final.

73. *Olmstead*, 277 U.S. at 465 ("The intervening wires are not part of his house or office any more than are the highways along which they are stretched.").

74. *Id*. at 466.

communications of American citizens, particularly in circumstances where scientific advancements provided government officials with new technological surveillance tools.[75] Justice Brandeis, in his dissent, warned:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[76]

Notwithstanding Justice Brandeis's pleas for the court to decide *Olmstead* in a manner that would provide for adaptation,[77] the Court focused on an inside-the-home/outside-the-home dichotomy and held that the telephone wires in this case were necessarily unprotected, as they extended outside the defendant's home and did not implicate any privacy concerns.[78]

It took the United States Supreme Court over forty years to overturn the *Olmstead* decision. In 1967, the Court was faced with a similar eavesdropping case in *Katz v. United States*.[79] The Justices took the opportunity to create what has remained the foundational analysis for searches conducted by agents of the government for more than forty years.[80]

---

75. *Id*. at 473 (Brandeis, J., dissenting). *See also* Kerr, *supra* note 15, at 1023-24 (discussing the "wrong turn" the Court made in *Olmstead*); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002) (noting that the *Olmstead* holding "symbolizes the Court's lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment").

76. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting). Justice Brandeis was eerily correct regarding the possibility that our private papers might somehow be revealed without the government physically intruding, and the science-fiction enthusiast in me cannot help wondering if his speculation regarding "[a]dvances in the psychic and related sciences" may someday, too, come to fruition. *Id.*

77. *Id*. at 472 ("Clauses guaranteeing to the individual protection against specific abuses of power, must have a . . . capacity of adaptation to a changing world."). For discussion of how the Court has adapted and shifted its understanding of Fourth Amendment principles in the face of ever-advancing technologies, see Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1748222##.

78. *Olmstead*, 277 U.S. at 464 (majority opinion).

79. 389 U.S. 347, 348 (1967).

80. Justice Harlan's test, explained in his concurrence, has been used repeatedly by the United States Supreme Court in a variety of different search contexts. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 88-91 (1998) (applying test to defendants who were at an apartment for short period of time for purpose of bagging cocaine); California v. Greenwood, 486 U.S. 35, 39-43 (1988) (applying test to garbage placed at the roadside); California v. Ciraolo, 476 U.S. 207, 211-15 (1986) (applying test to law enforcement's aerial surveillance of defendant's fenced-in backyard); Oliver v. United States, 466 U.S. 170, 177-81 (1984) (applying test to observation of marijuana plants by law enforcement officers who had trespassed on defendant's property).

Justice Harlan's *Katz* concurrence provides the foundation for analysis in his "reasonable expectation of privacy" test.[81] According to this analysis, Fourth Amendment protection attaches where a person has "exhibited an actual (subjective) expectation of privacy" and that expectation is "one that society is prepared to recognize as 'reasonable.' "[82] In *Katz*, the Court determined that an "electronic" intrusion may violate a citizen's Fourth Amendment right against unreasonable searches and seizures by the government.[83] Forty years later, we must ask ourselves if the analysis announced in *Katz* and applied to physical phone lines could potentially be expanded to apply to digital information. Is it possible that in the last forty years we have seen another paradigm shift, in which citizens should be permitted to assert a reasonable expectation of privacy in the contents of their mobile phones, much the same way *Katz* allowed the assertion of a privacy right in communications via physical phone line?

B. The Court's Lack of Foresight in Kyllo

In 2001, the Supreme Court made another attempt to apply the Fourth Amendment to a new technology when the Court decided *Kyllo v. United States*.[84] A law enforcement officer suspected Danny Kyllo was growing marijuana inside his home.[85] As part of their investigations, law enforcement officers used a device called the Agema Thermovision 210[86] The end result of the Court's decision in *Kyllo* is that the use of a thermal imaging device to learn that the defendant was growing marijuana inside his home was a search and was a violation of the Fourth Amendment because it was an intrusion into the personal and private sphere of the home[87]:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.[88]

81. *Katz*, 389 U.S. at 360-62 (Harlan, J., concurring).
82. *Id*. at 361.
83. *Id*. at 353 (majority opinion).
84. 533 U.S. 27 (2001).
85. *Id*. at 29.
86. *Id*.
87. *Id*. at 40.
88. *Id*. at 34-35 (citation omitted).

It is open to debate, however, whether this holding is a victory for privacy advocates or whether any positive value it may have is merely an illusion.[89] First of all, it is not likely that courts would apply this same reasoning in cases outside the context of the home, given the home's historically preferred status in Fourth Amendment law.[90] Further, the Court hinged its holding on the fact that the device used by law enforcement was not in general public use.[91] Presumably, if the device had been in general public use, the Court could have considered the heat differential coming off Kyllo's house the type of information one knowingly exposes to the public and in which one has no reasonable expectation of privacy.[92]

One need only imagine a relatively simple set of facts to see how *Kyllo* could be applied in a devastating manner to searches of mobile phones. Imagine you are riding in a car with a friend who, unbeknownst to you, is carrying a small amount of marijuana. Your friend's vehicle is stopped for a minor traffic infraction, which eventually leads to both of you being arrested for misdemeanor possession of a controlled substance. Law enforcement officers seize your mobile phone and wish to look at its contents, based on their understanding that evidence of drug transactions is regularly communicated via mobile phone. Being a privacy-conscious person, you have password protected your phone, and despite officers' efforts to obtain your password, you have remain tight-lipped. No worries. Given the wide availability to the general public of devices and processes used to either crack a password-protected phone[93] or copy data from a password protected phone,[94] the officer who uses one of

89. *See* Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, in CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE, 11, 15-16 (Jeffrey Rosen & Benjamin Wittes eds., 2011), *available at* http://books.google.com/ (search "Constitution 3.0"; then follow "Constitution 3.0: Freedom and Technological Center" hyperlink) (noting that "*Kyllo* places few limitations on the use of technology to spy on the populace," and calling the holding "little more than a pyrrhic victory for privacy advocates").

90. *See* LEGAL PAPERS OF JOHN ADAMS, *supra* note 11.

91. *Kyllo*, 533 U.S. at 34.

92. Under this analysis, the heat is akin to the trash left at the curbside in *California v. Greenwood*, 486 U.S. 35, 40-41 (1988) (holding that a person does not have a reasonable expectation of privacy in the contents of her trash).

93. *See* JONATHAN ZDZIARSKI, IPHONE FORENSICS: RECOVERING EVIDENCE, PERSONAL DATA & CORPORATE ASSETS (2008), *available at* http://books.google.com/ (search "iPhone Forensics"; then follow "IPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets" hyperlink).

94. *See Cellebrite Universal Forensics Extraction Device (UFED)*, CELLEBRITE, http://www.cellebrite.com/forensic-products.html#UFED (last visited July 1, 2012). Absent any special hacking or cracking device, researchers have demonstrated that even computers or mobile phones protected by full disk encryption are vulnerable to breach and capable of having their data copied and inspected. *See* Eoghan Casey et al., *The Growing Impact of Full Disk Encryption on Digital Forensics*, 8 DIGITAL INVESTIGATION 129 (2011); J. Alex Halderman et al., Lest We Remember: Cold Boot Attacks on Encryption Keys, in PROC. 2008 USENIX SECURITY SYMPOSIUM 45, 56, *available at* http://www.usenix.org/events/sec08/tech/full_papers/halderman/halderman.pdf

these devices is conceivably *not conducting a search*, under *Kyllo*. Where there is no search, there are no Fourth Amendment considerations. In this scenario, an officer can gain access to your private information simply because any member of the general public could do so.

There may not be a satisfactory resolution to these problems, however. Even if Justices truly understood these new technologies, the period of time it takes a case to reach the Supreme Court for review is likely to render rulings obsolete because such rulings would necessarily apply to obsolete technologies.[95]

III. CAN COURTS CRAFT A SOLUTION?

A. Conflicting Decisions Among State Courts and Courts of Appeals

The proliferation of mobile phones and the ever-increasing likelihood that a mobile phone will be discovered on an arrestee has caused struggle in state and lower federal courts due to the absence of a Supreme Court decision on the question.[96] Courts considering the question have reached wildly divergent results based on similar facts.[97] This is because courts have framed the issue in several different ways when announcing their decisions.[98]

(documenting extraction of data from fully encrypted device and finding that "a moderately skilled attacker can circumvent many widely used disk encryption products if a laptop is stolen while it is powered on or suspended").

95. *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (discussing largely obsolete pager technology).

96. *See supra* notes 3, 5, 8 and accompanying text; *see, e.g.*, United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008) (supporting the Fifth Circuit's decision in Finley that "if a cellphone is lawfully seized, officers may also search any data electronically stored in the device"); United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at *4 (E.D. Mo. Apr. 29, 2008) ("[T]he automobile exception allows the search of the cell phone just as it allows a search of other closed containers found in vehicles."); United States v. Lottie, No. 3:07cr51RM, 2008 WL 150046, at *3 (N.D. Ind. Jan.14, 2008) (finding a warrantless mobile phone search to be justified by exigent circumstances); United States v. Dennis, Criminal No. 07-008-DLB, 2007 WL 3400500, at *7 (E.D. Ky. Nov.13, 2007) (concluding that a search of a mobile phone incident to arrest no different from search of other evidence seized incident to arrest); United States v. Parada, 289 F. Supp. 2d 1291, 1303-04 (D. Kan. 2003) (holding that where mobile phone seized incident to arrest, exigent circumstances justified accessing mobile phone's record of calls because incoming calls might cause older calls to be overwritten).

97. *Compare* United States v. Finley, 477 F.3d 250 (5th Cir. 2007), *with* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573 at *7 (N.D. Cal. May 23, 2007).

98. *See, e.g.*, *Finley*, 477 F.3d at 260 n.7 (focusing on the fact that the mobile phone was on the arrestee's person, as opposed to simply within his immediate control); Hawkins v. State, 704 S.E. 2d 886, 891-92 (Ga. Ct. App. 2010) (acknowledging tremendous storage capacity of mobile phones and approving warrantless search where officer limited search to "a search for specific evidence of the crime for which Hawkins was arrested that the officer had good reason to believe was stored on the cell phone").

1. Finley *and* Park*: The Early Cases*

In 2007, the United States Court of Appeals for the Fifth Circuit threw down the gauntlet when it held that an officer could lawfully search the digital contents of the arrestee's mobile phone incident to his arrest.[99] *Finley* marked the first time a federal court of appeals had expressly approved a law enforcement officer's search of data stored on a mobile phone.[100] The opinion in *Finley* gave a terse analysis of a search of the arrestee's person incident to his arrest and flatly stated that the search was lawful under the Supreme Court's holdings in *Robinson* (defining the scope of the full search of a person to include containers) and *Belton* (defining container and approving the search of containers incident to arrest).[101] There was very little discussion of the matter and virtually no discussion of possible privacy implications.

In a factually similar case decided within months of *Finley*, a California federal court expressly rejected the reasoning of *Finley* and held that under *Chadwick* a search of a mobile phone that was in the arrestee's possession should be analyzed as a "possession[] within an arrestee's . . . control" and not as part of "the [arrestee's] person."[102] Based on that classification, the *Park* court contended that *Chadwick* requires law enforcement officers to obtain a warrant for a search of a mobile phone seized incident to a lawful arrest.[103] It appears that the *Park* court was trying to do the right thing, trying to find a way to protect citizens' private information; however, the *Park* court's attempt to protect citizens' information came at the cost of questionable reasoning. In its explanation as to *why* mobile phones should be classified as possessions within the arrestee's control rather than as part of a "full search of the person,"[104] the *Park* court rested its analysis on the large amount of private information that can be stored on the phone.[105] Accordingly, its holding is largely policy based; the court was concerned with the "far-ranging consequences" of allowing warrantless searches of mobile phones

99. *Finley*, 477 F.3d at 260 n.7. After law enforcement officers conducted a controlled buy of methamphetamine involving the defendant, he was lawfully arrested. *Id*. at 253-54. A special agent who was an expert in narcotics trafficking, "searched through the phone's call records and text messages." *Id*. at 254.

100. *Park*, 2007 WL 1521573, at *7 ("[T]he Court is aware of only one circuit court case on the issue" of "whether officers may search the contents of a cellular phone as a search incident to arrest.").

101. *Finley*, 477 F.3d at 259-60.

102. *Park*, 2007 WL 1521573, at *8.

103. *Id*.

104. United States v. Robinson, 414 U.S. 218, 235 (1973) (noting that it is well settled that a full search of the person is both an exception to the warrant requirement and a reasonable search).

105. *Park*, 2007 WL 1521573 at *8.

incident to arrest.[106] Policy implications are important when considering the private data of United States citizens; however, where United States Supreme Court precedent requires a particular outcome, it seems disingenuous for a court to force the outcome of a case by simply relying on public policy.

Additionally, though the court in *Park* attempted to describe its decision as in accord with Supreme Court precedent, it did so unconvincingly. The mobile phones in question were "removed from" the defendants after they had been transported to booking.[107] The *Park* court's strained attempt to analogize these mobile phones to the locked container in *Chadwick* only undermines the court's reasoning. A mobile phone discovered in the hand, in the pocket, or in another article of clothing that is actually on the defendant must necessarily be analyzed in the same manner as the pack of cigarettes in *Robinson*.[108] It is unfortunate that *Park* was the first answer to *Finley*. *Park*'s analysis is confused and clumsy; it does not provide a satisfactory roadmap for how courts can adhere to constitutional principles as described by the Supreme Court and at the same time protect the Fourth Amendment rights of citizens.

2. Courts Begin to Fall in Line Behind Finley

After the Court of Appeals for the Fifth Circuit finally spoke to the issue definitively in *Finley*, several state and federal courts fell in line.[109] It is easy to understand why: *Finley* is simple. The analysis does not require courts to face the inevitable and difficult question of privacy associated with searches of mobile phones. If an item can fit easily within the precedents of the United States Supreme Court, why should lower courts belabor the issue and attempt to forge new legal ground? These courts are precedent-bound to apply the Court's warrant exceptions faithfully, and most courts have followed *Finley*'s easy answer.

For example, in *United States v. Wurie*,[110] officers lawfully arrested Brima Wurie for distributing cocaine.[111] Officers observed that several calls on Wurie's caller ID screen had come from "my house."[112] Fortuitously, Wurie's mobile phone rang while it was in the

106. *Id*.
107. *Id*. at *2.
108. *Robinson*, 414 U.S. at 236 (holding that officer was entitled to inspect crumpled pack of cigarettes discovered on the arrestee's person incident to arrest).
109. *See, e.g.*, United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009) ("Decisions of district courts and Courts of Appeals (often analogizing cell phones to the earlier pager technology) trend heavily in favor of finding that the search incident to arrest or exigent circumstances exceptions apply to searches of the contents of cell phones.").
110. *Id*. at 104.
111. *Id*. at 106.
112. *Id*.

possession of officers, and they flipped the phone open.[113] When officers flipped the phone open, they saw that the call was coming from "my house" and saw a phone number.[114] Officers then cross referenced the number and obtained the address associated with that number.[115] The court held that "[t]he search of Wurie's cell phone incident to his arrest was limited and reasonable. The officers, having seen the 'my house' notation on Wurie's caller identification screen, reasonably believed that the stored phone number would lead them to the location of Wurie's suspected drug stash."[116]

Courts that have followed *Finley*'s lead tend to focus on the distinction between a search of items on the arrestee's person at the time of his arrest and those items merely in the arrestee's immediate control.[117] Those courts have also gone out of their way to mention that the quantity of information capable of storage on a mobile phone is not relevant to any consideration of whether a search of the phone's data is permissible.[118]

3. Flipping the Script on Finley

Is there any hope for privacy advocates after *Finley*? The courts that have questioned the search in *Finley* so far have come at it from a few different directions. Some courts have reasoned that a mobile phone does not fit *Belton*'s definition of a container.[119] Other courts have, in the context of an inventory search, held that a search of the contents of a mobile phone cannot be justified under the rationales advanced for the warrantless inventory search.[120] Additionally, a few courts have rejected the search of data on a mobile phone incident to arrest because it does not comport with the Supreme Court's original justifications for allowing a search of the arrestee contemporaneous to a lawful arrest.[121] Further, some courts have rejected the notion that exigent circumstances may justify a warrantless search of a mobile phone.[122]

---

113. *Id*.
114. *See id*.
115. *Id*. at 106-07.
116. *Id*. at 110.
117. *See, e.g.*, People v. Diaz, 244 P.3d 501, 505-06 (Cal. 2011) (describing the distinction as "the key question" in the case).
118. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); *Diaz*, 244 P.3d at 508. *But see* Smallwood v. State, 61 So. 3d 448, 461 (Fla. 1st DCA 2011) (discussing why the amount of information on the phone doesn't matter under Supreme Court precedent but suggesting that perhaps this is a legitimate concern).
119. *See infra* Part III.A.3(i).
120. *See infra* Part III.A.3(ii).
121. *See infra* Part III.A.3(iii).
122. *See infra* Part III.A.3(iv).

(i) A Mobile Phone is Not a Container

Although the analysis in *Finley* is tempting in its simplicity of application, several courts have recently acknowledged its shortcomings and have focused their analysis on the nature of a mobile phone. These courts have rejected the notion that a mobile phone is a "container."[123] The leading case in this respect is *State v. Smith*,[124] in which the Supreme Court of Ohio held that a mobile phone is not a closed container under the United State's Supreme Court's holding in *Belton*.[125] The *Finley* court did not expressly refer to a mobile phone as a container, but implied it through its reference to searches of containers under *Belton*.[126] A close examination of the language in *Belton* suggests that its analysis should only extend to containers that can contain physical objects.[127] Although a mobile phone is itself a physical object, the data stored on or in the phone is not contained in the manner contemplated by the Supreme Court in *Belton*. If one were to truly apply Belton's "container" definition to a mobile phone, *Belton* would permit an officer to open the battery door on the phone and remove the battery. *Belton* contemplates a physical opening of a closed container. Of course, *Belton* was decided in 1981, long before mobile phones were generally available to the public.[128]

(ii) An Inventory Search is Not an Investigation

One court facing the mobile-phone-search evaluated the search under the search-incident-to-arrest exception, the inventory exception, and the exigent circumstances exception.[129] The *Wall* court rejected all three rationales, but its discussion of the inventory justification offers some good advice for how attempted inventory searches of mobile phone data should be handled.[130] The court found that searching text messages was not a proper inventory search because it did not serve the rationales for the creation of the

123. *See supra* notes 56 & 57 and accompanying text for the *Belton Court's* definition of "container."

124. 920 N.E.2d 949 (Ohio 2009).

125. *Id*. at 954.

126. *See* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

127. The *Belton* Court's holding that officers may examine objects inside a container necessarily requires that the container be capable of holding "objects." New York v. Belton, 453 U.S. 454, 460 n.4 (1981). *See also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 57 (2008) ("[T]he search incident to arrest doctrine . . . has been framed with tangible physical evidence in mind.").

128. The first mobile phone call was placed by a Motorola Executive in 1973. GERARD GOGGIN, CELL PHONE CULTURE: MOBILE TECHNOLOGY IN EVERYDAY LIFE 29-30 (2006). Generally, wide availability of mobile phones to the public did not occur until the 1990s. *See* H. Lacohée, N. Wakeford & I. Pearson, *A Social History of the Mobile Telephone with a View of its Future*, BT TECH. J., July 2003 at 203, 205.

129. United States v. Wall, No. 08-60016-CR, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008).

130. *Id*. at *3-4.

inventory search exception to the warrant requirement: "to protect property from theft and the police from lawsuits based on lost or stolen property."[131] The court acknowledged that mobile phones could, of course, be inventoried, but noted that "there is no need to document the phone numbers, photos, text messages, or other data stored in the memory of a cell phone to properly inventory the person's possessions because the threat of theft concerns the cell phone itself, not the electronic information stored on it."[132] Although there is not presently any indication that law enforcement officers intend to justify mobile phone searches under the inventory warrant exception, the language and reasoning in *Wall* should serve as a guide for further analysis of these issues when they arise.

(iii) Searching Data on a Mobile Phone Incident to Arrest Does Not Further the Supreme Court's Justifications for the Search Incident to Arrest Doctrine

An additional tool courts may have in asserting that mobile phone searches incident to arrest should not be conducted absent a warrant is that such searches do not further the traditional goals of the search incident to arrest doctrine: officer safety and the preservation of evidence. In an opinion drafted prior to the Supreme Court's decision in *Gant*, the Middle District of Florida held that where Ariel Quintana was arrested for driving with a suspended license, an officer's search of his mobile phone was not a valid search incident to arrest.[133] After the officer placed Quintana under arrest, the officer noticed the smell of raw marijuana, but no marijuana was discovered inside the vehicle or on Quintana's person.[134] In an effort to further investigate the smell, the officer looked through photographs on Quintana's mobile phone, including a photograph "of an intimate nature involving a woman as well as a photo of marijuana plants in what he characterized as a marijuana 'grow house.' "[135] The court held that such a search "had nothing to do with officer safety or the preservation of evidence related to the crime of arrest," and "pushe[d] the search-incident-to-arrest doctrine beyond its limits."[136]

This wisdom became the law of the land when the United States Supreme Court decided *Arizona v. Gant*.[137] In *State v. Smith*, decided after *Gant*, the Ohio Supreme Court held that "the justifications behind allowing a search incident to arrest are officer safety and the

131. *Id.* at *4.
132. *Id.*
133. United States v. Quintana, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009).
134. *Id.* at 1295.
135. *Id.* at 1296.
136. *Id.* at 1300.
137. 556 U.S. 332 (2009).

preservation of evidence. There is no evidence that either justification was present in this case."[138] Notably, *Smith* was a drug-related case.[139] Generally, courts have held that drug-related cases present a high likelihood that evidence of the crime of arrest will be discovered on the arrestee's mobile phone and have largely permitted such searches.[140] The Ohio Supreme Court, however, held that an individual's privacy interest in the contents of his mobile phone required law enforcement officers to obtain a warrant prior to intruding into the mobile phone's contents even though the state's interest in collecting and preserving evidence justified its warrantless seizure.[141]

(iv) The Exigent Circumstances Rationale for Warrantless Pager-searches Incident to Arrest Should Not Extend to Mobile Phones

Before mobile phones were in the pockets of millions of Americans, there was the pager. Much of the case law that has emerged regarding searches of mobile phones is based on precedent that was based on searches of pagers. The United States Supreme Court has not directly ruled on a warrantless search of a pager incident to arrest,[142] but several Circuit Courts of Appeals have validated warrantless searches of pagers, citing exigent circumstances and the need to preserve evidence.[143] Some courts have distinguished pagers from mobile phones and have held that the line of cases dealing with

138. State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).

139. *Id*. at 950.

140. *See, e.g.*, People v. Diaz, 244 P.3d 501 (Cal. 2011).

141. *Smith*, 920 N.E. 2d at 955 ("Once the cell phone is in police custody, the state has satisfied its immediate interest in collecting and preserving evidence and can take preventive steps to ensure that the data found on the phone are neither lost nor erased. But because a person has a high expectation of privacy in a cell phone's contents, police must then obtain a warrant before intruding into the phone's contents.").

142. Mark Mayakis, *Comment, Cell Phone – A "Weapon" of Mass Discretion*, 33 CAMPBELL L. REV. 151, 156 (2010).

143. *See, e.g.*, United States v. Hunter, No. 96-4259, 1998 WL 887289, at *3 (4th Cir. Oct. 29, 1998) (upholding warrantless search of pager incident to arrest based on the possibility that evidence might be destroyed if no search occurred); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (noting that the information on a pager can be destroyed by turning off the device or touching a button and stating that "it is imperative that law enforcement officers have the authority to immediately 'search' or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence."); United States v. Stroud, No. 93-30445, 1994 WL 711908, at *2 (9th Cir. Dec. 21, 1994) ("[T]he pager was seized incident to a lawful arrest and searched to obtain evidence that might otherwise have been destroyed. This exigent circumstance combined with the lawful seizure destroyed [defendant's] reasonable expectation of privacy in the contents of his pager. In light of these facts, we find that the district court did not err by denying [defendant's] motion to suppress the pager evidence.").

pager searches is inapplicable in mobile phone search cases and therefore has no precedential value.[144]

But is there a possibility that mobile phone data could be destroyed in other ways, such as remote wiping?[145] Perhaps. But even if remote wiping were a widespread obstacle preventing officers from doing good and honest police work, Justice Werdegar, of the California Supreme Court, dispenses with this potential argument in her *Diaz* dissent when she points out that even where remote data wiping is possible, law enforcement can easily thwart such action simply by removing the phone's battery.[146]

4. Bound by Precedent?

For the privacy advocate, there are some signs that courts may be beginning to listen regarding our desire to protect the private information we store on our mobile devices. In a case currently before the Florida Supreme Court,[147] the First District Court of Appeal issued an opinion upholding a warrantless mobile phone search under the United States Supreme Court's precedents, but seriously questioning the soundness and wisdom of allowing such searches where there is no reasonable belief the phone contains evidence of the crime of arrest.[148] In *Smallwood*, the crime of arrest was armed robbery.[149] The court held that it was bound to determine this case pursuant to the United States Supreme Court's holding in *Robinson* and stated that "containers found upon a person incident to arrest may be searched without 'additional justification.' "[150] The Florida district court of appeal noted that *Gant* was not applicable as its holding only applied to searches incident to arrest in an automobile context.[151] The court found *Gant* "informative," however,[152] stating as follows:

> Were we free to do so, we would find, given the advancement of technology with regards to cell phones and other similar portable electronic devices, officers may only search cell phones incident to

144. *See, e.g.*, United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007) (discussing overwriting of data on pager and exigent circumstances justifying warrantless search of pager that do not exist for mobile phones).

145. *See, e.g.*, Melanie Barton Zoltán, *How to Wipe Your Phone Remotely*, PCWORLD (Nov. 3, 2010 1:30 PM), http://www.pcworld.com/article/209605/how_to_wipe_your_phone_remotely.html.

146. *Diaz*, 244 P.3d at 515 n.24 (Werdegar, J., dissenting).

147. *See Florida Supreme Court Docket, Case Number: SC11-1130*, FLORIDA SUPREME COURT, http://jweb.flcourts.org/pls/docket/ds_docket?p_caseyear=2011&p_casenumber=1130 (last visited July 1, 2012).

148. Smallwood v. State, 61 So. 3d 448, 459-62 (Fla. 1st DCA 2011).

149. *Id*. at 448.

150. *Id.* (quoting *United States v. Robinson*, 414 U.S. 218, 235 (1973)).

151. *Id*. at 462.

152. *Id*.

> arrest if it is reasonable to believe evidence relevant to the crime of arrest might be found on the phone. Here, there was no evidence the officer had such a reasonable belief.[153]

It appears that courts are beginning to recognize that we have a problem here that cannot be simply resolved under existing Supreme Court precedent. My hope is that more judges begin to step up, as Judge Wolf did in the *Smallwood* opinion, and ask for some clarification.

B. Some Proposed Solutions

American courts are bound by Supreme Court precedent,[154] but American law professors are not. Scholars have dedicated hundreds of pages of analysis to this problem in recent years.[155] Through these proposals, scholars attempt to craft a workable rule that affirms the privacy expectations citizens have for their personal information. But given the rapid advancement of mobile phone technology, it is clear that this exercise is fraught with difficulties.

Take, for example, a proposal discussed by Adam Gershowitz only four years ago.[156] Gershowitz noted that the mobile phone cases that had been decided at that point in time did not deal with searches that went very deep into the data on a phone.[157] Gershowitz explored a possible bright-line rule that might be a workable solution to the mobile phone search problem. He proposed that "courts could set a bright-line rule that police can take five steps, but no more, when rummaging through an iPhone's contents."[158] Gershowitz admits that this number is arbitrary but notes that its value would be in its ability to act as a clear rule law enforcement officers could follow with ease.[159] Under this proposal, an officer would be constitutionally permitted to take only five steps "into" the phone without obtaining a warrant.

The appeal of this approach is that it would solve some of the problems presented by a mobile phone's almost infinite capacity to "contain" data; the problem with this approach is that, unfortunately, it is already nearly obsolete only four years after it was proposed. Most mobile phones provide the user instant access to e-mail, social

---

153. *Id*.

154. State courts are free, of course, to provide in their state constitutional analogs more protection than the floor provided by the Fourth Amendment. *See, e.g.*, Cooper v. California, 386 U.S. 58, 62 (1967) (noting states have power to impose higher standards than those required by the federal Constitution).

155. *See, e.g.*, Gershowitz, *supra* note 127; Kerr, *supra* note 62; Solove, *supra* note 62.

156. Gershowitz, *supra* note 127. Professor Gershowitz notes that this proposal is likely to cause more problems than it solves, however. *Id*. at 54.

157. *Id*. at 41.

158. *Id*. at 54.

159. *Id*. at 55.

networking sites, and even in some instances bank information.[160] Applying this proposal to a mobile phone search in the age of smartphones would provide little protection of private information.

Professor Gershowitz has also explored the possibility that citizens might be able to protect their private information by locking their mobile phones with a password.[161] However, Gershowitz all but decimates this possibility by noting the wide availability of password-cracking techniques and devices law enforcement officers and members of the general public now have access to.[162] Gershowitz also explores the possibility that one might be protected by the Fifth Amendment in the event she is coerced into providing a password or otherwise provides the password involuntarily.[163] As he points out, the most notable thing about this inquiry is that in such a situation, Fifth Amendment protection would likely only attach where a criminal charge ensues.[164] This means that there may be no protection for the innocent person who is browbeaten into providing her mobile phone password to an overzealous law enforcement officer.[165]

Another notable privacy scholar, Daniel J. Solove, has suggested that the Supreme Court abandon the reasonable expectation of privacy test altogether.[166] Although this may seem quite extreme to some, it may be the only way to truly protect intimate information citizens clearly want protected. As Justice Scalia famously wrote, "[i]n my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, [reasonable expectations of privacy] . . . bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."[167]

---

160. Many banks now offer online banking specifically designed for mobile phone access. *See, e.g.*, *Mobile Banking FAQs*, REGIONS, http://www.regions.com/faq/mobile_banking.rf (last visited July 1, 2012); Mobile Banking FAQs, USBANK, http://www.usbank.com/mobile/mobilefaqs.html (last visited July 1, 2012); *Mobile Banking*, WELLS FARGO, https://www.wellsfargo.com/mobile/ (last visited July 1, 2012).

161. *See* Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1147-65 (2011).

162. *Id*. at 1164-65.

163. *Id*. at 1168.

164. *Id*. at 1173.

165. *Id*. ("In the event that police find no incriminating information on an arrestee's phone and do not bring criminal charges as a result of an arrestee turning over his password, there is a strong argument that truly innocent individuals have no civil-rights remedy because, under the Court's decision in *Chavez v. Martinez*, Fifth Amendment claims are limited to 'criminal cases.' ") (citing Chavez v. Martinez, 538 U.S. 760, 764-65 (2003) (plurality opinion)).

166. Solove, *supra* note 62, at 1524 ("Looking at expectations is the wrong inquiry. The law should protect certain information regardless of whether people expect it to be private or not.").

167. Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

Finally, Orin S. Kerr advocates for legislative intervention rather than judicial determination of issues on the cutting edge of technology.[168] However, it is not yet clear that legislatures have the will to write mobile phone protections into law. In 2011, the California State Legislature became the first state legislature to address the issue when the California State Assembly and the California State Senate sent SB 914[169] to California's Governor for his signature. This bill provided that "[t]he information contained in a portable electronic device shall not be subject to search by a law enforcement officer incident to a lawful custodial arrest except pursuant to a warrant issued by a duly authorized magistrate . . . ."[170] Governor Jerry Brown vetoed the bill, stating that the courts were better equipped to deal with search and seizure issues.[171] Orin Kerr noted that the Governor had it "exactly backwards."[172]

IV. MOBILE PHONE: MORE THAN A LAPTOP

Today's mobile phones are capable of doing the same things laptop and desktop computers are capable of. Arguably, mobile phones have the potential to reveal even more of an individual's private information, since the mobile phone is often carried everywhere, at all times. Furthermore, the mobile phone's ability to track and locate individuals raises serious concerns regarding potential government use or abuse. Given the vast amount of data accessible from a mobile phone, at the very least, courts should evaluate a mobile phone exactly the same way they would evaluate a laptop computer. A search for case law regarding warrantless searches of laptop computers incident to arrest did not return any results, possibly because law enforcement officers regularly seek and obtain warrants prior to conducting these searches. One Department of Justice manual explores the issue, suggests that the law is not settled, and instructs that in some instances the best practice may be to seize the computer and then obtain a warrant.[173]

It is clear to me that any analogy likening a mobile phone to an address book, a pager, or a physical container is superficial and detrimental. Mobile phones are more than this; they are repositories

168. Kerr, *supra* note 62, at 888.

169. S. 914, 2011 Leg., 2010-11 Reg. Sess. (Cal. 2011), *available at* http://leginfo.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_bill_20110902_enrolled.html.

170. *Id*.

171. David Kravets, *Calif. Governor Veto Allows Warrantless Cellphone Searches*, WIRED (Oct. 10, 2011, 11:09 AM), http://www.wired.com/threatlevel/2011/10/warrantless-phone-searches/.

172. *Id*.

173. H. MARSHALL JARRETT ET AL., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 33-34 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

for our private thoughts, much like locked diaries. In the spirit of the Fourth Amendment's protection of papers and effects, law enforcement officers should respect the privacy of United States citizens and defer to a neutral and detached magistrate empowered to issue warrants to make the choice regarding whether or not to search.

Courts seem confused,[174] but users do not. Users of mobile phones fiercely advocate for privacy and security in the personal information accessible via their mobile phones.[175] This is evidence that mobile phone users have exhibited a subjective expectation of privacy in the contents of their mobile phones. It is almost a laughable notion that this expectation is one that society is not prepared to recognize as reasonable (to speak in the language of *Katz*[176]). It is time the courts recognized and respected mobile phone users' privacy by requiring law enforcement officers seek and obtain a warrant prior to rummaging around in the private world contained on our mobile phones.

174. *See* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. 2007) ("[T]he line between cell phones and personal computers has grown increasingly blurry . . . ."); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (refusing to classify mobile phones as either address books or computers).

175. For evidence of this, simply look to the recent scandals surrounding Carrier IQ and the News of the World phone hacking scandal. *See* Adrian Kingsley-Hughes, *Carrier IQ 'May Have' Collected Text Messages*, ZDNET (Dec. 14, 2011, 3:58 AM), http://www.zdnet.com/blog/hardware/carrier-iq-may-have-collected-text-messages/17122; Indu Chandrasekhar et al., *Phone Hacking: Timeline of the Scandal*, TELEGRAPH, http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html (last visited July 1, 2012).

176. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).