

# Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?

Adam M. Gershowitz\*

*ABSTRACT: Over the last few years, dozens of courts have authorized police to conduct warrantless searches of cell phones when arresting individuals. Under the “search incident to arrest” doctrine, police are free to search text messages, call histories, photos, voicemails, and a host of other data if they arrest an individual and remove a cell phone from his pocket. Given that courts have offered little protection against cell-phone searches, this Article explores whether individuals can protect themselves by password protecting their phones. The Article concludes, unfortunately, that password protecting a cell phone offers minimal legal protection when an individual is lawfully searched incident to arrest. In conducting such a search, police may attempt to hack or bypass a password. Because cell phones are often found in arrestees’ pockets, police may take the phones to the police station, where computer-savvy officers will have the time and technology to unlock a phone’s contents. And if police are unable to decipher the password, they may request or even demand that an arrestee turn over his password, without any significant risk of suppression of evidence found on the phone under the Miranda doctrine or the Fifth Amendment’s Self-Incrimination Clause. In short, while password protecting a cell phone may make it more challenging for police to find evidence, the password itself offers very little legal protection to arrestees. Accordingly, legislative or judicial action is needed to narrow the search-incident-to-arrest doctrine with respect to cell phones.*

I. INTRODUCTION.....	1128
II. THE SEARCH-INCIDENT-TO-ARREST DOCTRINE .....	1131

---

\* Associate Professor of Law, University of Houston Law Center. An earlier version of this Article was presented at faculty workshops at The Florida State University College of Law and Stetson University College of Law. I am grateful to Susan Brenner, Sandra Guerra Thompson, Wayne Logan, and George Thomas for helpful suggestions, and to Dave Brucker and Lauren Serice for valuable research assistance.

A.	<i>THE SUPREME COURT'S "STANDARD" SEARCH-INCIDENT-TO-ARREST DOCTRINE</i> .....	1132
B.	<i>SEARCHING CELL PHONES INCIDENT TO ARREST</i> .....	1135
1.	The Vast Majority of Lower Court Cases Have Upheld the Search Incident to Arrest of Cell Phones .....	1136
2.	A Smaller Number of Cases Have Relied on Varied Rationales in Rejecting the Search of Cell Phones Incident to Arrest .....	1139
C.	<i>THE BIG PICTURE: WHERE THE LAW CURRENTLY STANDS AND WHAT IS LIKELY TO OCCUR IN THE NEAR FUTURE</i> .....	1142
1.	The Current State of the Law and Practice of Searching Cell Phones Incident to Arrest.....	1143
2.	New Directions in the Law and Private Responses to the Problem.....	1144
a.	<i>The Supreme Court Could (But Likely Will Not) Curb Broad Police Power To Search Cell Phones</i> .....	1144
b.	<i>Legislative Efforts To Curb Warrantless Cell-Phone Searches Are Nonexistent</i> .....	1146
c.	<i>Individual Efforts: Password Protecting Cell Phones</i> .....	1147
III.	CAN POLICE ATTEMPT TO BREAK INTO A PASSWORD-PROTECTED PHONE?.....	1147
A.	<i>PASSWORD PROTECTING A PHONE DOES NOT CLOAK IT IN IMPENETRABLE FOURTH AMENDMENT PROTECTION AND PREVENT ALL WARRANTLESS SEARCHES</i> .....	1148
B.	<i>POLICE CAN SEARCH LOCKED CONTAINERS INCIDENT TO ARREST</i> .....	1150
1.	Searching Locked Physical Containers.....	1151
2.	Searching a Locked (Password-Protected) Phone Is Permissible.....	1153
C.	<i>ATTEMPTS TO BREAK PASSWORDS MUST BE CONTEMPORANEOUS WITH ARREST</i> .....	1154
1.	Different Rules for Searching Items Associated with the Person and Items That Are Merely Nearby Possessions ....	1155
2.	Cell Phones Will Often Be Items Associated with the Person, Giving Police a Lengthy Time To Search .....	1158
3.	If Cell Phones Are Merely Possessions, How Long Can Police Spend Searching Them Before the Search Ceases To Be Contemporaneous? .....	1161
4.	Will Police Have Enough Time To Crack the Password?..	1163
IV.	THE IPHONE MEETS THE FIFTH AMENDMENT .....	1165
A.	<i>THE MIRANDA DOCTRINE MAY PROTECT AGAINST REQUESTS FOR PASSWORDS, BUT VIOLATIONS WILL NOT LEAD TO THE SUPPRESSION OF VALUABLE EVIDENCE</i> .....	1166

B. *POLICE DEMANDS FOR THE PASSWORD LIKELY DO NOT AMOUNT TO A VIOLATION OF THE FIFTH AMENDMENT'S SELF-INCRIMINATION CLAUSE*..... 1168

V. CONCLUSION ..... 1174

## I. INTRODUCTION

Over the last decade, cell-phone use has exploded. Most Americans now use cell phones capable of containing huge amounts of information, such as pictures, documents, music, text messages, and e-mails.<sup>1</sup> Not surprisingly, the fact that cell phones are carried in public and hold enormous amounts of data has made them attractive targets for law enforcement. Numerous defendants have been convicted of drug dealing<sup>2</sup> and child pornography based on evidence found on cell phones.<sup>3</sup>

In an earlier article, I explained how, under the search-incident-to-arrest doctrine, police can conduct warrantless searches of cell phones when they arrest suspects for practically any offense.<sup>4</sup> So long as police have a valid reason to arrest a suspect, and in the course of doing so find a cell phone on his person or immediately nearby, the search-incident-to-arrest doctrine permits police to search the arrestee's phone, even if there is no reason to believe the phone contains evidence related to the arrest.<sup>5</sup> The only significant restriction on the search of cell phones incident to arrest is that the search must be conducted close in time to the arrest—i.e., “contemporaneously” with the arrest.<sup>6</sup>

---

1. See Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 41 (2008).

2. See, e.g., *United States v. Fuentes*, 368 F. App'x 95, 98–99 (11th Cir. 2010) (per curiam) (rejecting an argument to suppress contact information appearing in the cell phone of a drug dealer); *United States v. Young*, 278 F. App'x 242 (4th Cir. 2008) (per curiam) (affirming reliance on a cell phone's text messages to convict a defendant of heroin distribution and sentence him to 420 months incarceration); *United States v. Wurie*, 612 F. Supp. 2d 104 (D. Mass. 2009) (upholding a conviction for intent to distribute crack based on call-log information on a cell phone); *United States v. Santillan*, 571 F. Supp. 2d 1093 (D. Ariz. 2008) (relying on a cell phone's call history to link a defendant to a marijuana distribution ring); *United States v. Valdez*, No. 06-CR-336, 2008 WL 360548 (E.D. Wis. Feb. 8, 2008) (denying motion to suppress use of a cell phone address book and call history to demonstrate that the defendant had been in contact with others in a drug conspiracy); *People v. Shepard*, No. Ho32876, 2008 WL 4824083, at \*1 (Cal. Ct. App. Nov. 7, 2008) (upholding conviction where police officer “looked at the text messages in the cell phone because he knew that ‘cell phones are used to facilitate drug transactions’”); *People v. Diaz*, 81 Cal. Rptr. 3d 215 (Ct. App. 2008) (upholding a drug conviction based on a text message stating “6 4 80,” which referred to the sale of six ecstasy pills for eighty dollars).

3. See, e.g., *Brady v. Gonzalez*, No. 08 C 5916, 2009 WL 1952774 (N.D. Ill. July 2, 2009) (finding a picture of a nude child on a cell phone); *United States v. McCray*, No. CR408-231, 2009 WL 29607 (S.D. Ga. Jan. 5, 2009) (denying suppression of child pornography found on a cell phone); *Lemons v. State*, 298 S.W.3d 658 (Tex. Ct. App. 2009) (rejecting effort to suppress pornographic picture of fourteen-year old girl found on a cell phone).

4. Gershowitz, *supra* note 1.

5. See *id.* at 44.

6. See *id.* at 39.

Although it is far from a routine practice, the number of cell-phone searches incident to arrest has recently risen dramatically.<sup>7</sup> Over the last few years, more than forty courts have been called on to assess the constitutionality of searching cell phones incident to arrest; and the vast majority of those courts have approved the practice.<sup>8</sup>

With so little judicial protection against warrantless cell-phone searches, this Article explores whether individuals can protect their cell-phone data by password protecting their phones. The value of password protecting the phone depends on the answer to three crucial questions. First, when police arrest a suspect and encounter a password-protected phone, can they attempt to break the password themselves and unlock the phone without the consent of the arrestee and without a search warrant? Second, how long can police tinker with the phone in an effort to gain access to its contents? And third, if police cannot crack the password on their own, can they request or even demand that the arrestee turn over the password without violating the *Miranda* doctrine or the Fifth Amendment protection against self incrimination?

The first question is relatively straightforward, as set forth in Part II, which reviews the search-incident-to-arrest doctrine and examines caselaw predating the Internet<sup>9</sup> that permits police to break into and search containers incident to arrest.<sup>10</sup> Courts have regularly upheld searches where police have unlocked or broken into locked glove compartments, briefcases, and even safes during searches incident to arrest.<sup>11</sup> Accordingly, there is a strong argument that, incident to a lawful arrest, police should be permitted to unlock the cell phone so long as they can figure out the password in a short period of time following arrest. This should be disconcerting to the millions of Americans who use simplistic passwords (such as “1234” or their birthday)<sup>12</sup> that police can easily guess. And it should be particularly

---

7. See *infra* notes 62–66 and accompanying text (recounting the growing number of cases where police have searched cell phones incident to arrest as well as under the automobile exception, inventory exception, exigency exception, and pursuant to consent).

8. See *infra* note 66 and accompanying text.

9. Professor Orin Kerr has made a compelling argument that courts should seek a “technology-neutral” translation of Fourth Amendment issues to the Internet. See Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010).

10. See *infra* Part III.B.1.

11. See *infra* notes 128–35 and accompanying text.

12. See Ashlee Vance, *If Your Password's Still 123456, It Might as Well Be HackMe*, N.Y. TIMES, Jan. 21, 2010, at A1 (explaining that the most popular password is “123456” and that “one out of five Web users still decides to leave the digital equivalent of a key under the doormat: they choose a simple, easily guessed password like ‘abc123,’ ‘iloveyou’ or even ‘password’ to protect their data” (internal quotation marks omitted)).

worrisome to iPhone users, whose devices have weak password-protection functions that are vulnerable to tampering.<sup>13</sup>

The second question—how long police can take in an effort to decipher or bypass the password?—is more complicated. Part III addresses this question. In an “ordinary” search incident to arrest, officers must conduct the search contemporaneously to arrest. Although there is no fixed time limit, courts require police to conduct such searches as soon as practicable, and judges rarely tolerate lengthy, drawn-out searches. This limitation is deceiving, however, in the context of cell-phone searches. U.S. Supreme Court precedent provides that when police search for an item associated with the person of an arrestee, such as his clothing or wallet, they can take far longer to conduct the search and can comfortably do so at the station house, rather than at the scene of the arrest. When a cell phone is found in an arrestee’s pocket or attached to his belt, a compelling argument exists that the phone is associated with the arrestee’s person and thus that the police have hours to try to break the password—including by use of computer-hacking software at the police station.

The final question—whether police can ask or demand that an arrestee reveal or enter his password—also demonstrates how little protection arrestees have in the information contained in their cell phones. In most cases, before requesting a cell-phone password, police should be obligated to read the arrestee his *Miranda* rights.<sup>14</sup> Yet, failure to read the warnings will not result in suppression of any illegal evidence found on the cell phone because the fruit-of-the-poisonous-tree doctrine never applies to *Miranda* violations.<sup>15</sup>

If police demanded (rather than requested) that an arrestee disclose his password, the arrestee would have only a very weak argument that the police have compelled a testimonial response in violation of the Fifth Amendment’s Self-Incrimination Clause. Moreover, even if the self-incrimination privilege theoretically existed in this context, few criminal defendants would be savvy enough to invoke the protection. And innocent individuals who have nothing illegal on their phones (and thus no evidence to suppress) will be unable to bring civil-rights lawsuits because recent Supreme Court caselaw limits Fifth Amendment remedies to “criminal cases,” and is not applicable to situations where the police find no evidence and the arrestee is not charged.<sup>16</sup> Part IV discusses these Fifth Amendment implications for police requests or demands for the password to an arrestee’s phone.

---

13. See *infra* notes 197–200 and accompanying text (describing how the iPhone’s password-protection function is much less sophisticated than that of some other smart phones).

14. *Miranda v. Arizona*, 384 U.S. 436 (1966).

15. See *infra* note 214 and accompanying text.

16. See *infra* notes 243–48 and accompanying text.

This Article paints a grim picture of the privacy of arrestees' cell phones. Police have wide authority to search phones incident to arrest, even if the arrest has nothing to do with the phone itself and even if the phone is password-protected. Because cell phones are typically found on an arrestee's person, Supreme Court precedent seemingly gives police authority to spend hours trying to crack the password at the scene or in the comfort of the police station. Additionally, because many Americans choose overly simplistic passwords and certain cell phones are easily hacked, there is a chance that police can break into the phone without any help from the arrestee. If police request the password from the arrestee, the *Miranda* doctrine provides only nominal protection because defendants rarely invoke it and police violation of the rule does not result in the suppression of evidence. Only if police demand that an arrestee provide his password can he make out a plausible (though still debatable) Fifth Amendment claim.

Because even password protecting a cell phone does not provide a significant roadblock to a police search of the phone incident to arrest, this Article concludes that there is a strong need for judicial or legislative intervention to curb the search-incident-to-arrest doctrine for cell-phone searches.

## II. THE SEARCH-INCIDENT-TO-ARREST DOCTRINE

The Supreme Court has recognized a host of scenarios in which police can search people or places without a warrant.<sup>17</sup> Perhaps the most common exception police invoke is the search-incident-to-arrest exception.<sup>18</sup> Under this exception, police are authorized to search the person and his immediate "grabbing space" to protect against physical danger and to prevent the destruction of evidence. In doing so, police can search in any area or container near the arrestee, including a pocket, a purse, and even a wallet. In Part II.A below, I briefly review five key Supreme Court cases that establish the broad contours of the search-incident-to-arrest doctrine. Part II.B then discusses the dozens of lower-court decisions that have applied the search-incident-to-arrest doctrine to cell phones. Thereafter, Part II.C provides a big-picture overview of the rules and standards for searching cell phones incident to arrest and looks at how the Supreme Court, legislatures, and individual cell-phone users may shape the law in the coming years.

---

17. See Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473-74 (1985) (listing "over twenty exceptions to the probable cause or the warrant requirement or both"); see also *California v. Acevedo*, 500 U.S. 565, 582-83 (1991) (Scalia, J., concurring in the judgment) (noting that at least two more exceptions to the warrant requirement have been added since Professor Bradley's article).

18. 3 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 5.2(b), at 99 (4th ed. 2004) (describing the search incident to arrest as probably the most common type of police search).

## A. THE SUPREME COURT'S "STANDARD" SEARCH-INCIDENT-TO-ARREST DOCTRINE

Although it is not the earliest search-incident-to-arrest case,<sup>19</sup> the starting point for today's broad search-incident-to-arrest doctrine is the Supreme Court's 1969 decision in *Chimel v. California*.<sup>20</sup> In *Chimel*, the Court suppressed evidence police found when they searched Chimel's entire home, including his attic and garage, following his arrest for burglary.<sup>21</sup> Despite suppressing the evidence, the *Chimel* decision provided broad authority for the police to search incident to arrest. The Court held that, contemporaneous with a lawful arrest, police could search for weapons that an arrestee could use against the arresting officer and to prevent an arrestee from concealing or destroying evidence.<sup>22</sup> The Court limited the scope of this search to the arrestee's person and the area within his immediate control.<sup>23</sup> Thus, while police could not rummage through Chimel's entire house following his arrest, they were free to search anywhere on his person or within his immediate grabbing space.

A few years after *Chimel*, in *United States v. Robinson*, the Court moved a step further and clarified that police could open closed containers when searching incident to arrest.<sup>24</sup> Police arrested Robinson for operating a motor vehicle with a revoked license.<sup>25</sup> During a search incident to arrest of Robinson's person, the arresting officer felt an object in Robinson's coat pocket but was unsure of what it was.<sup>26</sup> The officer reached into the pocket and pulled out a "crumpled up cigarette package."<sup>27</sup> Still unsure what was in the package, the officer opened it and discovered capsules of heroin.<sup>28</sup> Even though Robinson was not initially arrested for a drug crime and the officer had no reason to believe the package in his pocket contained drugs, the Supreme Court upheld the search.<sup>29</sup> The Court announced a bright-line rule for searches incident to arrest, permitting police officers to open and search through all items on an arrestee's person, even if they are in a closed container, and even without suspicion that the contents of the container are

---

19. For a discussion of the earlier search-incident-to-arrest cases, see James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417, 1422 (tracing the history of the doctrine from *Weeks v. United States*, 232 U.S. 383 (1914), and *Carroll v. United States*, 267 U.S. 132 (1925)).

20. 395 U.S. 752 (1969).

21. *Id.* at 754.

22. *Id.* at 763.

23. *See id.*

24. 414 U.S. 218 (1973).

25. *Id.* at 220.

26. *Id.* at 223.

27. *Id.* (internal quotation marks omitted).

28. *Id.*

29. *Id.* at 236.

illegal.<sup>30</sup> Put differently, the Court in *Robinson* clarified that the search-incident-to-arrest doctrine is automatic, and that courts should not conduct a case-by-case inquiry to determine whether police were actually suspicious or whether the search was truly necessary to protect the officer or prevent the destruction of evidence.<sup>31</sup>

In its next series of important search-incident-to-arrest decisions, the Supreme Court turned its attention to automobiles. In *New York v. Belton*, the Court expanded its bright-line rule to permit searches incident to arrest of the entire interior of automobiles (although not the trunk) following a valid arrest.<sup>32</sup> In *Belton*, the officer stopped a car for speeding and, upon smelling marijuana, arrested the occupants.<sup>33</sup> With the occupants safely removed from the vehicle, the officer then searched the passenger compartment of the car and found a jacket in the backseat.<sup>34</sup> The officer unzipped the pockets of the jacket and found cocaine.<sup>35</sup> In upholding the search of the jacket, the Court explained the value of “a straightforward rule, easily applied, and predictably enforced.”<sup>36</sup> To make matters simple and predictable, the Court permitted police, following a lawful arrest, to search the entire passenger compartment of a vehicle and to open any container inside the vehicle, regardless of whether it could possibly contain a weapon or evidence of a crime.<sup>37</sup>

In 2004, the Court expanded police authority to search vehicles by authorizing the search incident to arrest of vehicles that were recently used by an arrestee.<sup>38</sup> In *Thornton*, police arrested Thornton for drug possession after he parked his vehicle and walked away from it.<sup>39</sup> After handcuffing Thornton, the officer walked over to Thornton’s vehicle, searched the passenger compartment, and found a handgun that was later used to support a charge of possessing a firearm in furtherance of a drug-trafficking crime.<sup>40</sup> The Court upheld the search and thus expanded the search-incident-to-arrest doctrine to permit a search of the passenger compartment of a vehicle if the arrestee recently occupied it.<sup>41</sup>

---

30. *Id.* at 235–36.

31. *See id.* at 235.

32. 453 U.S. 454 (1981).

33. *Id.* at 455–56.

34. *Id.* at 456.

35. *Id.*

36. *Id.* at 459.

37. *See id.* at 460–61. The Court did not clarify in *Belton*, nor has it in any subsequent cases, whether locked containers in an automobile can be opened incident to arrest.

38. *Thornton v. United States*, 541 U.S. 615 (2004).

39. *Id.* at 617–18.

40. *Id.* at 618–19.

41. *Id.* at 622–24.

While the decision in *Thornton* expanded the search-incident-to-arrest doctrine, it raised the ire of Justice Scalia, who concurred in the judgment only and maintained that the Court had stretched the doctrine “beyond its breaking point.”<sup>42</sup> Justice Scalia argued that the search-incident-to-arrest doctrine should be scaled back to allow searches of the passenger compartment of a vehicle only when “it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.”<sup>43</sup>

Only a few years later in *Arizona v. Gant*,<sup>44</sup> a majority of the Court partially embraced Justice Scalia’s position. In *Gant*, police arrested the defendant for driving with a suspended license, handcuffed him, and placed him in the back of a police car.<sup>45</sup> Thereafter, police searched Gant’s vehicle and found a jacket in the backseat that contained cocaine.<sup>46</sup> Under *Belton*, the Court should have upheld the search of Gant’s vehicle and the jacket in the backseat. The Court instead used *Gant* as an opportunity to significantly narrow the *Belton* decision and the scope of police authority to search vehicles incident to arrest. First, the Court held that police can only search a vehicle to protect their safety if “the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search.”<sup>47</sup> Second, the Court adopted Justice Scalia’s position from *Thornton* and held that police can search the passenger compartment of a vehicle incident to arrest “when it is ‘reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.’”<sup>48</sup>

While the *Gant* decision is clearly an effort to narrow the search-incident-to-arrest doctrine, it is debatable how much change it will foster. On the one hand, in cases like *Gant*’s where the arrestee is already handcuffed and the reason for the arrest was a traffic infraction (for which no evidence could be found in the vehicle), a search of the vehicle is impermissible. On the other hand, many traffic stops immediately produce some evidence of other illegal activity (such as the odor of drugs in the vehicle)<sup>49</sup> that will authorize a search under *Gant*.<sup>50</sup> Thus, while some vehicle searches incident to arrest are now prohibited under *Gant*, it is not

---

42. *Id.* at 625 (Scalia, J., concurring in the judgment).

43. *Id.* at 632.

44. 129 S. Ct. 1710 (2009).

45. *Id.* at 1714.

46. *Id.*

47. *Id.* at 1719.

48. *Id.* (quoting *Thornton*, 541 U.S. at 632 (Scalia, J., concurring in the judgment)).

49. For example, we need look no further than the Court’s decision in *Belton* itself, where the initial traffic stop led to an officer smelling marijuana. See *supra* note 33 and accompanying text.

50. Moreover, in a likely small number of cases, police who desire to search a vehicle incident to arrest may be willing to take a safety risk and begin to search while the arrestee is still within grabbing distance of the vehicle.

yet clear just how many fewer searches will occur<sup>51</sup> or whether, in the next few years, the Supreme Court will expand *Gant* to restrict nonvehicle searches incident to arrest, such as the cigarette pack in *Robinson*.<sup>52</sup>

\* \* \*

While many questions remain unanswered after the Court's 2009 decision in *Gant* and while that decision may ultimately lead to a significant narrowing of the search-incident-to-arrest doctrine, at present, the doctrine continues to give law enforcement enormous power. Incident to an arrest, police may search the person of an arrestee and his immediate grabbing space. In many instances, police can search the passenger compartment of an arrestee's vehicle. And when conducting searches incident to arrest of persons, their grabbing space, and their vehicles, police are permitted to open and search containers. It is this broad authority that arguably gives police the power to search cell phones incident to arrest.

#### B. SEARCHING CELL PHONES INCIDENT TO ARREST

As wireless technology has become ubiquitous, courts have been called on to apply the search-incident-to-arrest doctrine to digital devices. The first such cases appeared in the mid-1990s and involved very simple pagers and beepers that stored only phone numbers and short messages. Courts universally upheld the search incident to arrest of such devices. For example, in *United States v. Chan*, police activated a pager and retrieved telephone numbers that linked Chan to a drug ring.<sup>53</sup> The federal court upheld the search of Chan's pager because it considered a pager an electronic container, and Supreme Court precedent authorized the search of containers incident to arrest.<sup>54</sup> The court further explained that it was irrelevant that the arrestee could not retrieve a weapon from the pager or plausibly destroy any evidence from the pager.<sup>55</sup> Put simply, the court embraced the search-incident-to-arrest doctrine's bright-line rule for wireless technology and saw no reason to distinguish pagers from traditional searches of luggage, boxes, and other containers. In the years after *Chan*, half a dozen other courts upheld similar searches of pagers.<sup>56</sup>

---

51. One possibility is that police will reduce the number of searches incident to arrest and instead attempt to acquire evidence by impounding the vehicles and conducting inventories.

52. See Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 209 (2010) (discussing the possibility of *Gant*'s extension beyond automobiles); see also *infra* note 89 (discussing two cases where courts have refused to permit searches of cell phones incident to arrest because no evidence related to the suspect's original crime could be found on the phone).

53. 830 F. Supp. 531, 533 (N.D. Cal. 1993).

54. *Id.* at 534-35.

55. *Id.* at 535-36.

56. *United States v. Hunter*, No. 96-4259, 1998 WL 887289, at \*3 (4th Cir. Oct. 29, 1998) (per curiam) (upholding retrieval of telephone numbers from a pager); *United States v. Ortiz*,

1. The Vast Majority of Lower Court Cases Have Upheld  
the Search Incident to Arrest of Cell Phones

In the years following the *Chan* decision, cell-phone use increased dramatically in the United States. Early-generation cell phones were not markedly different than pagers, but they did contain additional data such as outgoing call logs and text messages. Law-enforcement officers quickly recognized that drug dealers could use cell phones to text their drug transactions without having to speak on the phone.<sup>57</sup> Accordingly, police began to search cell phones incident to arrest, and, beginning in the mid-2000s, courts were called on to assess the constitutionality of such searches.

Although it is impossible to know how many times police have searched cell phones incident to arrest in recent years, the number is likely in the thousands.<sup>58</sup> In many instances, police likely found no incriminating evidence,<sup>59</sup> and, in cases where police did find evidence related to a crime, defendants likely pled guilty without challenging the constitutionality of the searches.<sup>60</sup> Nevertheless, more than fifty defendants have challenged the warrantless search of early-generation cell phones over the last few years.<sup>61</sup> In a handful of cases, courts have addressed whether these warrantless searches were permissible under the automobile exception,<sup>62</sup> the inventory

84 F.3d 977, 984 (7th Cir. 1996) (same); *United States v. Stroud*, No. 93-30445, 1994 WL 711908, at \*2 (9th Cir. Dec. 21, 1994) (same); *United States v. Diaz-Lizaraza*, 981 F.2d 1216, 1222-23 (11th Cir. 1993) (inserting batteries and reactivating beeper so that it may be called after arrest is permissible); *United States v. Reyes*, 922 F. Supp. 818, 833-34 (S.D.N.Y. 1996) (upholding retrieval of telephone numbers from a pager); *United States v. Lynch*, 908 F. Supp. 284, 287-89 (D.V.I. 1995) (same).

57. *See, e.g.*, *People v. Shepard*, No. Ho32876, 2008 WL 4824083, at \*1 (Cal. Ct. App. Nov. 7, 2008) (quoting detective who testified that he “looked at the text messages in the cell phone because he knew that ‘cell phones are used to facilitate drug transactions, and that’s via text messages’”).

58. *See United States v. Chappell*, Crim. No. 09-139 (JNE/JJK), 2010 WL 1131474, at \*4 (D. Minn. Jan. 12, 2010) (rejecting claim that cell phone could be searched under inventory exception and noting testimony of police officer that “it was his understanding that he could inspect anything on the cellular phone without a warrant until the completion of the booking process”), *adopted by* 2010 WL 1131473 (D. Minn. Mar. 22, 2010); *United States v. Wall*, No. 08-60016-CR, 2008 WL 5381412, at \*4 (S.D. Fla. Dec. 22, 2008) (noting that a drug-enforcement agent testified during a suppression hearing that “it is his practice to search cell phones for text messages primarily because DEA’s policy allows for it and because it is common to find text messages that further the investigation”), *aff’d*, 343 F. App’x 564 (11th Cir. 2009) (per curiam).

59. *See, e.g.*, Scott J. Upright, Note, *Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment*, 51 WM. & MARY L. REV. 291, 292 & n.6 (2009) (noting how customs officials repeatedly searched and seized the cell phone of a Muslim firefighter whenever he reentered the United States).

60. *See Gershowitz, supra* note 1, at 40 n.84.

61. *See infra* notes 62-66.

62. The automobile exception allows police to conduct a warrantless search of a vehicle provided they have probable cause to believe evidence will be found in the vehicle. *See, e.g.*, *United States v. Monson-Perez*, No. 4:09CR623 HEA, 2010 WL 889833, at \*6-7 (E.D. Mo. Mar. 8, 2010) (concluding there was probable cause to search cell phone and allowing warrantless

exception,<sup>63</sup> the exigency exception,<sup>64</sup> or based on consent.<sup>65</sup> However, courts have decided the bulk of warrantless cell-phone search cases under the search-incident-to-arrest doctrine, and they have upheld the searches in the vast majority of cases.<sup>66</sup>

---

search under automobile exception); *United States v. Rocha*, No. 06-40057-01-RDR, 2008 WL 4498950, at \*6 (D. Kan. Oct. 2, 2008) (finding probable cause to search cell phone for drug activity and relying on automobile exception); *United States v. James*, No. 1:06CR134CDP, 2008 WL 1925032, at \*7 (E.D. Mo. Apr. 29, 2008) (upholding search of cell phone's call log based on automobile exception); *United States v. Fierros-Alvarez*, 547 F. Supp. 2d 1206, 1211-14 (D. Kan. 2008) (upholding search of cell phone located in vehicle under the automobile exception because inventory of vehicle turned up drugs and there was probable cause to believe the cell phone had facilitated drug transactions); *People v. Chho*, No. Ho34693, 2010 WL 1952659, at \*4 (Cal. Ct. App. May 17, 2010) (upholding search of text messages on repeatedly ringing cell phone under automobile exception); *State v. Boyd*, 992 A.2d 1071, 1090 (Conn. 2010) (upholding search of cell phone under automobile exception), *cert. denied*, No. 10-7287 (U.S. Feb. 22, 2011); *State v. Novicky*, No. Ao7-0170, 2008 WL 1747805, at \*6 (Minn. Ct. App. Apr. 15, 2008) (upholding search of cell phone seized from an automobile when search was conducted on the day of trial).

63. The inventory exception allows an administrative cataloging of items found in an impounded vehicle, thus making it possible to find a cell phone, but difficult to justify searching its contents. *See Chappell*, 2010 WL 1131474, at \*14 (rejecting Government's contention that search of cell phone during the booking process was permissible under the inventory exception); *Wall*, 2008 WL 5381412, at \*3 (same).

64. Exigency searches authorize warrantless police activity to prevent the destruction of evidence, escape of suspects, or to deal with danger to the suspect or the community. *See United States v. Salgado*, No. 1:09-CR-454-CAP-ECS-5, 2010 WL 3062440, at \*4 (N.D. Ga. June 12, 2010) (upholding warrantless search of cell phone because "the data on the phone could have been altered, erased, or deleted remotely"), *adopted by* 2010 WL 3035755 (N.D. Ga. July 30, 2010).

65. Consent searches can be conducted without probable cause or a warrant so long as police obtain permission to search the area freely and voluntarily. *See James*, 2008 WL 1925032, at \*4 (upholding search of cell phone's call log based on consent and the automobile exception); *United States v. Galante*, No. 94 Cr. 633 (LMM), 1995 WL 507249, at \*3 (S.D.N.Y. Aug. 25, 1995) (concluding that consent to search a vehicle also provided consent to search cellular phone inside the vehicle); *Lemons v. State*, 298 S.W.3d 658, 662 (Tex. App. 2009) (finding consent to search cell phone for pictures when police asked for permission to search phone and defendant responded by handing the phone to the officers).

66. *United States v. Pineda-Areola*, 372 F. App'x 661, 663 (7th Cir. 2010) (explaining that dialing the phone number associated with an arrestee is not a search, but that even if it were, it would be permissible to search the phone of an arrestee incident to arrest); *United States v. Fuentes*, 368 F. App'x 95, 99 (11th Cir. 2010) (per curiam) (approving search incident to arrest of cell phone, though not conducting thorough analysis of the issue); *Silvan W. v. Briggs*, 309 F. App'x 216, 225 (10th Cir. 2009) ("[T]he permissible scope of a search incident to arrest includes the contents of a cell phone found on the arrestee's person."); *United States v. Murphy*, 552 F.3d 405, 410-12 (4th Cir. 2009) (upholding search incident to arrest of cell phone and rejecting argument that phones with larger storage capacity should be treated differently than early-generation cell phones); *United States v. Young*, 278 F. App'x 242, 246 (4th Cir. 2008) (per curiam) (denying motion to suppress text messages found incident to arrest); *United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007); *United States v. Faller*, 681 F. Supp. 2d 1028, 1046 (E.D. Mo. 2010) (upholding search of cell phone because, even though search was not authorized by warrant being executed, police inevitably would have arrested defendant and would have been entitled to search the phone incident to arrest);

The most prominent case upholding the search of a cell phone incident to arrest is the Fifth Circuit's decision in *United States v. Finley*.<sup>67</sup> After arresting Finley as part of a staged drug sale, police searched the cell phone

---

Newhard v. Borders, 649 F. Supp. 2d 440, 448–49 (W.D. Va. 2009) (noting that the Fourth Circuit approves searching cell phones incident to arrest and granting officers qualified immunity for doing so); Brady v. Gonzalez, No. 08 C 5916, 2009 WL 1952774, at \*3 (N.D. Ill. July 2, 2009) (concluding, though without performing a thorough analysis, that police may examine the contents of a cell phone incident to arrest); 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.”); United States v. Quintana, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009) (suppressing incriminating photos of drug activity found after an arrest for driving with a suspended license because the search was unrelated to the reason for arrest, but noting that if a “defendant is arrested for drug-related activity, police may be justified in searching the contents of a cell phone for evidence related to the crime of arrest”); United States v. McCray, No. CR408-231, 2009 WL 29607 (S.D. Ga. Jan. 5, 2009) (upholding search incident to arrest of cell phone for child pornography after arrest for statutory rape); United States v. Santillan, 571 F. Supp. 2d 1093, 1104 (D. Ariz. 2008) (upholding search of cell phone’s call history); United States v. Gates, Criminal No. 08-42-P-H, 2008 WL 5382285, at \*13 (D. Me. Dec. 19, 2008) (upholding search incident to arrest of cell phone that occurred “within minutes” of arrest); United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008) (“[I]f a cellphone is lawfully seized, officers may also search any data electronically stored in the device.”); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at \*3 (E.D. Wis. Feb. 8, 2008) (upholding search of cell phone’s address book and call log incident to arrest, though noting that “we can leave for another day the propriety of a broader search equivalent to the search of a personal computer”); United States v. Curry, Criminal No. 07-100-P-H, 2008 WL 219966, at \*8–10 (D. Me. Jan. 23, 2008) (upholding search of cell phone’s call log for calls from drug informant); United States v. Dennis, Criminal No. 07-008-DLB, 2007 WL 3400500, at \*7–8 (E.D. Ky. Nov. 13, 2007) (upholding search of cell phone’s call history under search-incident-to-arrest doctrine); United States v. Lottie, No. 3:07-cr-51-AS, 2007 WL 4722439 (N.D. Ind. Oct. 12, 2007) (upholding search of cell phone primarily on exigency grounds but arguably under the search-incident-to-arrest exception as well); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1279 (D. Kan. 2007) (upholding search of cell phone for numbers of outgoing and incoming calls); United States v. Murphy, No. 1:06CR00062, 2006 WL 3761384 (W.D. Va. Dec. 20, 2006) (upholding search of cell phone’s text messages), *aff’d*, 552 F.3d 405; United States v. Diaz, No. CR 05-0167 WHA, 2006 WL 3193770, at \*4 (N.D. Cal. Nov. 2, 2006) (upholding recording of names and numbers in address book and recording messages); United States v. Zamora, No. 1:05 CR 250 WSD, 2006 WL 418390, at \*5 (N.D. Ga. Feb. 21, 2006) (upholding search of cell phone for numbers of outgoing and incoming calls); United States v. Brookes, No. CRIM 2004-0154, 2005 WL 1940124, at \*3 (D.V.I. June 16, 2005) (upholding search of numbers in cell phone and pager); United States v. Cote, No. 03CR271, 2005 WL 1323343, at \*6 (N.D. Ill. May 26, 2005) (upholding search of cell phone’s call log, phone book, and wireless web inbox); United States v. Parada, 289 F. Supp. 2d 1291, 1303–04 (D. Kan. 2003) (upholding search of stored numbers to prevent destruction of evidence); State v. Harris, No. 1 CA-CR 07-0810, 2008 WL 4368209, at \*4 (Ariz. Ct. App. Sept. 23, 2008) (upholding search of photographs on cell phone); People v. Shepard, No. Ho32876, 2008 WL 4824083 (Cal. Ct. App. Nov. 7, 2008) (upholding search of cell phone’s text messages incident to arrest); People v. Diaz, 81 Cal. Rptr. 3d 215, 218 (Ct. App. 2008) (upholding search of cell phone ninety minutes after arrest and rejecting argument that cell phones should receive more attention because they are “capable of storing vast amounts of private information”).

67. 477 F.3d 250.

in his pocket incident to arrest.<sup>68</sup> Officers found incriminating text messages related to drug trafficking,<sup>69</sup> and Finley was subsequently convicted.<sup>70</sup>

On appeal, Finley contended that the search of his cell phone was unlawful because the Fourth Amendment permitted only the seizure, and not the warrantless search, of his phone.<sup>71</sup> Just as in the pager context, the Fifth Circuit refused to draw a distinction between wireless technology and searches of more traditional containers.<sup>72</sup> Citing familiar Supreme Court cases—*United States v. Robinson* and *New York v. Belton*<sup>73</sup>—the court explained 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.”<sup>74</sup> In short, the Fifth Circuit did not recognize any conceptual difference between searching physical containers for drugs and searching electronic equipment for digital information.

The *Finley* decision remains the most prominent case upholding the search of cell phones incident to arrest, but it is far from the only one. Approximately thirty other courts have agreed with the reasoning in *Finley* and upheld searches of cell phones incident to arrest.<sup>75</sup>

## 2. A Smaller Number of Cases Have Relied on Varied Rationales in Rejecting the Search of Cell Phones Incident to Arrest

Although the *Finley* decision is repeatedly cited as the leading case on the search incident to arrest of early-generation cell phones, a small number of courts have refused to follow its reasoning.<sup>76</sup> These courts have employed a variety of rationales in rejecting warrantless searches of cell phones.

---

68. *Id.* at 253–54.

69. *Id.* at 254–55. One incoming text message said, “So u wanna get some frozen agua,” a common term for methamphetamine. Another text message said, “Call Mark I need a 50,” a likely reference to asking for fifty dollars worth of narcotics. *Id.* at 254 n.2 (internal quotation marks omitted).

70. *Id.* at 255.

71. *Id.* at 260.

72. *See id.*

73. *See supra* notes 24–37 and accompanying text.

74. *Finley*, 477 F.3d at 259–60.

75. *See supra* note 66.

76. *United States v. McGhee*, No. 8:09CR31, 2009 WL 2424104, at \*3 (D. Neb. July 21, 2009) (relying on *Gant* and concluding that search of cell phone incident to arrest was unjustified because no evidence related to the crime of arrest (which occurred in early 2008) could be found in the phone when the arrest occurred in 2009); *United States v. Quintana*, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009) (rejecting search incident to arrest of cell phone’s photos because defendant was arrested for driving with a suspended license and no information of that crime could be found on a cell phone); *United States v. Wall*, No. 08-60016-CR, 2008 WL 5381412, at \*3–4 (S.D. Fla. Dec. 22, 2008) (finding that search was not contemporaneous and was not justified by exigent circumstances or inventory exception), *aff’d*, 343 F. App’x 564

The Ohio Supreme Court, in a recent and closely divided four-to-three opinion, is the most prominent court to reject searches of cell phones incident to arrest.<sup>77</sup> In *State v. Smith*, the police executed a controlled drug buy in which text messages and call records from the arrestee's phone confirmed his involvement in the drug sale.<sup>78</sup> Unlike the Fifth Circuit panel in *Finley*, the Ohio Supreme Court refused to accept the crucial premise that cell phones are just like any other container that might hold other objects. The four-justice majority maintained that to be considered a container within the meaning of the Supreme Court's decision in *Belton*, the item must be capable of holding a "physical object within it."<sup>79</sup> Because cell phones hold only intangible data, they could not be containers. Moreover, the majority ruled that the search-incident-to-arrest doctrine should not apply to cell phones because even basic cell phones "are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container."<sup>80</sup> The court thus authorized police to seize a cell phone incident to arrest but demanded that police obtain a warrant before "intruding into the phone's contents."<sup>81</sup>

---

(11th Cir. 2009) (per curiam); *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573, at \*8 (N.D. Cal. May 23, 2007) (rejecting search incident to arrest conducted at station because cell phones are possessions within arrestees' immediate control and cannot be searched at the station); *United States v. Lasalle*, Cr. No. 07-00032 SOM, 2007 WL 1390820 (D. Haw. May 9, 2007) (finding that search was not contemporaneous); *Commonwealth v. Diaz*, No. ESCR 2009-00060, 2009 WL 2963693, at \*6 (Mass. Super. Ct. Sept. 3, 2009) (rejecting search of cell phone incident to arrest because it occurred more than twenty minutes after arrest and was therefore not contemporaneous); *State v. Novicky*, No. A07-0170, 2008 WL 1747805, at \*4-5 (Minn. Ct. App. Apr. 15, 2008) (rejecting argument that search of cell phone held in evidence since initial arrest could fall under search-incident-to-arrest exception when search was conducted on the day of trial); *State v. Smith*, 124 Ohio St. 3d 163, 2009-Ohio-6426, 920 N.E.2d 949 (holding that cell phones are not containers that can be searched incident to arrest). Two other courts have intimated that searches of cell phones incident to arrest should be impermissible, without deciding the issue. See *United States v. James*, No. 1:06CR134 CDP, 2008 WL 1925032, at \*10 n.4 (E.D. Mo. Apr. 29, 2008) (noting in dicta, and without analysis, that even though search of cell phone was proper under a warrant, the district court judge disagreed with the magistrate's conclusion that the search was also justified under the search-incident-to-arrest doctrine); *United States v. Carroll*, 537 F. Supp. 2d 1290, 1299 (N.D. Ga. 2008) (expressing skepticism of search incident to arrest of a BlackBerry when a suspect surrendered at the police station, but ordering further briefing before deciding the issue). Finally, the Wisconsin Supreme Court recently rejected the warrantless search of a cell phone's picture gallery, but solely analyzed the issue under the exigent-circumstances and plain-view doctrines, without contemplating whether the evidence would be admissible under the search-incident-to-arrest doctrine. See *State v. Carroll*, 2010 WI 8, ¶¶ 21-42, 322 Wis. 2d 299, 778 N.W.2d 1.

77. See *Smith* ¶ 29.

78. See *id.* ¶ 4.

79. *Id.* ¶ 20.

80. *Id.* By contrast, the dissenting justices found the breadth of information held by cell phones irrelevant and saw no distinction between the search of a physical address book and the search of a cell phone's contacts page. See *id.* ¶ 34 (Cupp, J., dissenting).

81. *Id.* ¶ 23 (majority opinion).

A federal district judge in California offered a different rationale for rejecting the search incident to arrest of cell phones. In *United States v. Park*, police arrested the defendant on drug charges and brought him to the police station.<sup>82</sup> Approximately ninety minutes following the arrest, the police searched his cell phone at the station house and located incriminating information.<sup>83</sup> Like the Ohio Supreme Court, the *Park* court focused on the “immense amounts of private information” that can be stored on cell phones, explaining that “address books, calendars, voice and text messages, email, video, and pictures” could reveal “highly personal information.”<sup>84</sup> However, the *Park* court did not reject the idea that cell phones were containers. Rather, the court asserted that cell phones “should not be characterized as an element of [an] 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.’”<sup>85</sup>

The *Park* court pointed to a famous Supreme Court case—*United States v. Chadwick*—in which the Court rejected the search incident to arrest of a large footlocker that had been transported to the police station. The *Chadwick* decision seemed to draw a distinction between searches of the person—such as clothing and pockets—and searches of possessions within an arrestee’s immediate control—such as a footlocker.<sup>86</sup> According to the *Park* court’s interpretation of the *Chadwick* decision, items associated with the person of the arrestee can be searched at the scene or later at the police station, but items within the arrestee’s immediate control can only be searched incident to arrest at the scene, and not later at the police station.<sup>87</sup> Because the search incident to arrest of Park’s cell phone occurred at the station, it was therefore impermissible.<sup>88</sup>

At least two other federal courts have offered a third rationale for suppressing searches of cell phones by looking to the Supreme Court’s recent decision in *Arizona v. Gant*.<sup>89</sup> In *Gant*, the Supreme Court restricted

82. No. CR 05-375 SI, 2007 WL 1521573, at \*2 (N.D. Cal. May 23, 2007).

83. *Id.* at \*3-4.

84. *Id.* at \*8.

85. *Id.* at \*9 (second and third alterations in original) (quoting *United States v. Manclavo-Cruz*, 662 F.2d 1285, 1290 (9th Cir. 1981)).

86. *Id.* at \*8 (citing *United States v. Chadwick*, 433 U.S. 1, 16 n.10 (1977)).

87. *Id.* at \*6-7.

88. *See id.* at \*9. As I describe in more detail in Part III.C.2, the *Park* reasoning is unpersuasive. Nevertheless, the decision does have its defenders. *See Orso*, *supra* note 52, at 204-06 (advocating a coding-content distinction, but finding the *Park* decision consistent with Supreme Court precedent); Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165, 1200 (2008).

89. *United States v. McGhee*, No. 8:09CR31, 2009 WL 2424104, at \*3 (D. Neb. July 21, 2009) (relying on *Gant* and concluding that search of cell phone incident to arrest was unjustified because no evidence related to the crime of arrest (which occurred in early 2008) could be found in the phone when the arrest occurred in 2009); *United States v. Quintana*, 594 F. Supp. 2d 1291, 1300-01 (M.D. Fla. 2009) (rejecting search of cell phone’s photos incident

searches of automobiles incident to arrest to situations in which “the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search”<sup>90</sup> or “when it is ‘reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.’”<sup>91</sup> The Court’s decision in *Gant* was clearly limited to searches of automobiles incident to arrest, but these district courts evidently believed that the Court’s logic extended (or should be extended in the future) to cell phones as well.

Finally, a number of courts have suppressed evidence found in searches of cell phones incident to arrest on the grounds that the search was not contemporaneous with the arrest. For example, in *Commonwealth v. Diaz*, the arrestee’s cell phone repeatedly rang while he was being booked at the police station.<sup>92</sup> After four or five calls, an officer answered the phone and heard the caller attempt to buy drugs.<sup>93</sup> Relying in part on the fact that the officer answered the phone twenty minutes after arrest, a Massachusetts court suppressed evidence of the phone call because it occurred too long after arrest to be contemporaneous.<sup>94</sup> In *United States v. Lasalle*, a federal district judge grappled with a much lengthier time gap when police searched a cell phone at least two hours (and possibly up to four hours) after officers arrested the suspect.<sup>95</sup> Importantly, these contemporaneousness cases limit, but do not outrightly forbid, the search of cell phones incident to arrest.<sup>96</sup>

C. *THE BIG PICTURE: WHERE THE LAW CURRENTLY STANDS AND  
WHAT IS LIKELY TO OCCUR IN THE NEAR FUTURE*

As Part II.B demonstrates, a growing body of caselaw grapples with the searches of cell phones incident to arrest. Although it is relatively early in

to arrest because defendant was arrested for driving with a suspended license and no information of that crime could be found on a cell phone); *see also* *United States v. McCray*, No. CR408-231, 2009 WL 29607, at \*4 n.4 (S.D. Ga. Jan. 5, 2009) (upholding limited search of cell phone following arrest for statutory rape but noting that “[t]his case . . . does not present the question of whether a cell phone (a kind of computer capable of storing vast amounts of data) may be subjected to a comprehensive search incident to a defendant’s arrest for a simple traffic violation”).

90. *Arizona v. Gant*, 129 S. Ct. 1710, 1719 (2009).

91. *Id.* (quoting *Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in the judgment)).

92. No. ESCR 2009-00060, 2009 WL 2963693, at \*2 (Mass. Super. Ct. Sept. 3, 2009).

93. *Id.*

94. *Id.* at \*6.

95. Cr. No. 07-00032 SOM, 2007 WL 1390820, at \*7 (D. Haw. May 9, 2007).

96. In addition to *Diaz* and *Lasalle*, a federal court in Florida also found a warrantless search of a cell phone incident to arrest unconstitutional because it was conducted at the station and not contemporaneously with arrest. *United States v. Wall*, No. 08-60016-CR, 2008 WL 5381412, at \*3 (S.D. Fla. Dec. 22, 2008), *aff’d*, 343 F. App’x 564 (11th Cir. 2009) (per curiam). The *Wall* court did not specify how long after arrest the search was conducted.

the development of this area of law, Part II.C.1, below, draws several big-picture conclusions on the state of the law. Part II.C.2 then explores whether a Supreme Court decision or legislative activity will have any effect on law enforcement's ability to search cell phones incident to arrest in the near future.

### 1. The Current State of the Law and Practice of Searching Cell Phones Incident to Arrest

Although the issues surrounding the search incident to arrest of cell phones are still evolving, several things are clear. First, the number of cases addressing the issue is on the rise, suggesting that the number of searches by police on patrol may also be on the rise. While courts decided only six cases involving searches of cell phones incident to arrest between 2003 and 2006,<sup>97</sup> an additional thirty-one decisions were handed down from 2007 through the middle of 2010.<sup>98</sup> Over the last few years, more than a dozen additional courts have addressed searches of cell phones under the automobile exception, the inventory doctrine, exigency, and consent rationales.<sup>99</sup>

Second, most courts to address the constitutionality of searching cell phones incident to arrest have upheld the practice. At present, roughly thirty courts have approved cell-phone searches incident to arrest under the logic that police can search any container on an arrestee, including digital containers.<sup>100</sup>

Third, although a handful of cases suppressed evidence found through searches of cell phones incident to arrest, most of those courts did not outrightly reject the practice in all circumstances. Most courts that have suppressed evidence found through searches of cell phones incident to arrest have done so on the grounds that the search occurred too long after the arrest to be contemporaneous.<sup>101</sup> Indeed, in the most cited case rejecting the search of cell phones incident to arrest—*United States v. Park*—the court did not rule that cell phones could never be searched incident to arrest.<sup>102</sup> Rather, the *Park* court simply rejected the search under the particular facts of that case. To date, of the approximately forty cases to

---

97. See *supra* note 66.

98. See *supra* note 66.

99. See *supra* notes 62–65.

100. See *supra* Part II.B.

101. See *supra* notes 92–96 and accompanying text.

102. No. CR 05-375 SI, 2007 WL 1521573, at \*8 (N.D. Cal. May 23, 2007); see also *United States v. Curry*, Criminal No. 07-100-P-H, 2008 WL 219966, at \*9 (D. Me. Jan. 23, 2008) (discussing the *Park* decision and noting that “[t]he *Park* court deemed cell phones analogous instead to possessions within an arrestee’s control (such as closed containers or luggage) that lawfully may be searched without a warrant only if the search is ‘substantially contemporaneous’ with the arrest”).

address the search incident to arrest of a cell phone,<sup>103</sup> only a single case—the Ohio Supreme Court’s decision in *State v. Smith*—has expressly forbid the search of cell phones incident to arrest.<sup>104</sup>

Fourth, when courts have addressed whether the search of a cell phone was contemporaneous with arrest, their decisions have been far from uniform. For example, police searched two unrelated defendants (who ironically were both named Diaz) incident to their respective arrests in Massachusetts and California. In the Massachusetts case, the court found a search twenty minutes after arrest too late to be contemporaneous.<sup>105</sup> By contrast, the California court found a search that occurred ninety minutes after arrest perfectly acceptable.<sup>106</sup>

Finally, although the vast majority of cases have involved early-generation cell phones, rather than smart phones, the trend of the law strongly indicates that courts will reach the same results when cases involving iPhones, BlackBerries, and other advanced cell phones reach the courts, since in approving the search incident to arrest of cell phones, courts have rejected the argument that cell phones should be treated differently simply because they can hold large amounts of private data.<sup>107</sup>

## 2. New Directions in the Law and Private Responses to the Problem

Having sketched the current state of police authority to search cell phones incident to arrest, the harder task is to predict whether there will be any major changes in the law moving forward. Change could occur through any of three avenues: (1) the Supreme Court could narrow the search-incident-to-arrest doctrine; (2) state legislatures could impose statutory restrictions on police authority to search the cell phones of arrestees; or (3) cell-phone users could password protect their phones and shift the legal issues into more complicated Fourth and Fifth Amendment territory. I consider each of these possibilities in turn.

### *a. The Supreme Court Could (But Likely Will Not) Curb Broad Police Power To Search Cell Phones*

It is possible that the Supreme Court will grant certiorari in the next few years to rule on the constitutionality of searching cell phones incident to

---

103. See *supra* note 66.

104. See *State v. Smith*, 124 Ohio St. 3d 163, 2009-Ohio-6426, 920 N.E.2d 949.

105. Commonwealth v. Diaz, No. ESCR 2009-0060, 2009 WL 2963693 (Mass. Super. Ct. Sept. 3, 2009).

106. See *People v. Diaz*, 81 Cal. Rptr. 3d 215 (Ct. App. 2008).

107. United States v. Murphy, 552 F.3d 405 (4th Cir. 2009) (rejecting the argument that smart phones should be treated differently than ordinary phones because there is no standard for separating large-capacity from small-capacity phones, and information contained within larger-capacity phones could still be volatile and disappear while police get a warrant).

arrest.<sup>108</sup> While the vast majority of lower court cases have approved the search incident to arrest of cell phones, there is still a split of authority.<sup>109</sup>

If the Court was inclined to limit or prevent the search of cell phones incident to arrest, it could do so in two ways. First, the Court could agree with the Ohio Supreme Court that cell phones are not containers and require police to obtain warrants to search their contents. Given that cell phones regularly contain evidence of criminal activity that can be quickly destroyed (even from remote locations), it is unlikely the Court would take this approach. Second, and more plausibly, the Court could expand its recent decision in *Arizona v. Gant* beyond the automobile context and limit searches incident to arrest to those scenarios where police are likely to find evidence related to the reason for the arrest. Presently, police can still search a cigarette package in an arrestee's shirt pocket when the driver is arrested for driving with a suspended license, but police cannot search the arrestee's glove compartment or cigarette package if the arrestee has already been restrained.

In its search-incident-to-arrest jurisprudence, the Court has long endorsed bright-line rules that will be workable for police on the street. If after a few years of experience, the *Gant* rule proves workable, it will not be surprising to see the Court apply the same rationale to searches of arrestees. The *Gant* rule would seemingly reduce the number of cell-phone searches conducted incident to arrest because for most crimes (such as traffic offenses, murder, rape, and robbery), any potential evidence contained in an arrestee's cell phone will not be related to the reason for arrest.

On the other hand, there is reason to be less optimistic about the *Gant* solution. First, the Court may simply refuse to extend *Gant* to nonvehicle searches incident to arrest. The Court could conclude that when arresting individuals, there is always a need to search the arrestee to prevent the destruction of evidence or the risk of violence. To maintain a bright-line rule, the Court may be unwilling to delineate the circumstances in which some cell-phone searches are permissible and others are not.

Second, even if the Court does extend the *Gant* doctrine to cell phones, there is no telling when that will happen. Justice Scalia made a strong case for limiting the search incident to arrest of vehicles in his 2004 concurrence in *Thornton v. United States*; yet the Court did not adopt his position until five years later in *Gant*.

---

108. Following the Ohio Supreme Court's decision rejecting the search incident to arrest of cell phones, the Supreme Court of the United States requested a response to the Government's petition for certiorari. See Docket, SUPREME COURT U.S., <http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/09-1377.htm>. Although the Supreme Court ultimately denied the petition for certiorari, *State v. Smith*, 131 S. Ct. 102 (2010), the request for briefing may indicate that at least one member of the Court has some interest in the question.

109. See *supra* notes 66–96 and accompanying text.

Third, even if the *Gant* rule seemingly forbids many cell-phone searches, police can find ways to circumvent the rule. Police might (albeit on thinner grounds) arrest a traffic violator for a drug offense, rather than only for driving with a suspended license. The officer might testify that the car smelled of marijuana or that the defendant appeared glassy eyed and under the influence of illegal drugs.<sup>110</sup> Because cell phones are recognized tools of the drug trade and drug dealers regularly use text messages to communicate, police could plausibly claim a phone contains evidence related to the drug arrest. Of course, I do not mean to suggest that police will always be able to find ways around the *Gant* rule. But it is wise to remember that police officers (and the lawyers who train them about search and seizure) have long found ways to circumvent Supreme Court rules limiting their authority to search and investigate.<sup>111</sup>

In sum, while it is possible that the *Gant* doctrine will drastically reduce the number of cell-phone searches conducted incident to arrest, the Court must first adopt that doctrine and do so in a way that prevents clever law-enforcement officers from evading the rule. The prospects of that occurring in the near future are uncertain, to say the least.

*b. Legislative Efforts To Curb Warrantless Cell-Phone Searches Are Nonexistent*

Regardless of whether the Supreme Court restricts the search-incident-to-arrest doctrine, state legislatures could restrict searches of cell phones by amending their codes of criminal procedure. For instance, over three decades ago, the Massachusetts legislature codified a much more restrictive version of the search-incident-to-arrest doctrine because it believed the Supreme Court granted far too expansive authority to law enforcement to search arrestees.<sup>112</sup>

However, the prospect of legislatures taking steps to specifically narrow police authority to search cell phones is extremely unlikely. Despite the dozens of cases involving warrantless searches of cell phones over the last

---

110. The officer might also slow down the traffic stop and wait for a drug-sniffing dog that could provide a positive alert for drugs, thus allowing an arrest on drug charges.

111. See Donald Dripps, *The Fourth Amendment, The Exclusionary Rule, and the Roberts Court: Normative and Empirical Dimensions of the Over-Deterrence Hypothesis*, 85 CHL-KENT L. REV. 209, 238 (2010) (“[T]here is substantial evidence tending to show that police professionalism actually increases the risk that the police will exploit weaknesses in the remedial scheme by violating substantive Fourth Amendment rights for the sake of incriminating evidence. The exclusionary rule gives cities and departments an incentive to train their forces, but the training the police receive seems to be more concerned with admissibility than with legality.”).

112. See MASS. GEN. LAWS ch. 276, § 1 (2008) (“A search conducted incident to an arrest may be made only for the purposes of seizing fruits, instrumentalities, contraband and other evidence of the crime for which the arrest has been made, in order to prevent its destruction or concealment; and removing any weapons that the arrestee might use to resist arrest or effect his escape. Property seized as a result of a search in violation of the provisions of this paragraph shall not be admissible in evidence in criminal proceedings.”).

decade, the author is unaware of a single proposed bill to restrict such searches, or even a solitary legislative hearing to investigate the increasingly common practice.<sup>113</sup>

It is, of course, possible that a legislator will become interested in the practice and hold hearings on warrantless cell-phone searches. It is even possible that a legislator could drum up enough support to pass a law restricting searches of cell phones incident to arrest. But such a turn of events is unlikely to occur in a single state, and almost certainly will not occur in a sufficient number of states to effect any serious change in the current nationwide practice. If past is prologue, the prospect of legislative action is almost nil.

*c. Individual Efforts: Password Protecting Cell Phones*

With Supreme Court intervention uncertain, and legislative protection unlikely, protection against searches incident to arrest is left to cell-phone users themselves. Because the very purpose of cell phones is their convenience, users obviously will not leave them at home or store them in the trunk of their cars where they will be safe from the search-incident-to-arrest doctrine.<sup>114</sup> The only plausible option is for users to password protect their phones. Although early-generation cell phones did not come equipped with user-friendly password systems, popular smart phones on the market today—including iPhones, BlackBerries, and Droids—contain password features that enable users to restrict access to the phones' contents.

Without question, password protecting a phone makes it considerably harder for the police to search it incident to arrest. But it does not make it impossible. Parts III and IV below consider whether police can attempt to crack passwords and, if they are unable to do so, whether they can request or demand that an arrestee provide his password as part of the search-incident-to-arrest process.

III. CAN POLICE ATTEMPT TO BREAK INTO A PASSWORD-PROTECTED PHONE?

Assuming that cell-phone users opt to password protect their phones, the first important question is whether police can attempt to decipher and enter the password to access data on the phone. The answer to this question seems to be “yes.” Importantly, simply password protecting a phone does not

---

113. A Westlaw search of “bill or law or legislation or rule or propos! w/10 limit or restrict or curtail or reduce w/10 search w/10 ‘cell phone’” in the ALL NEWS database turns up only two articles, both of which involved the tangential issue of a single school district’s new policy restricting cell phone searches by teachers. Deb Kollars, *Student Wins Fight over Cell Phone Privacy*, SACRAMENTO BEE, Apr. 18, 2008, 2008 WLNR 7299431; Scott Smith, *Cell Text Snooping Draws Ire: Linden School Changes Policy After Incident*, RECORD (Stockton), Apr. 18, 2008, 2008 WLNR 7288213.

114. Ordinarily, police cannot search the trunk of a vehicle incident to arrest. See *New York v. Belton*, 453 U.S. 454, 461 n.4 (1981).

cloak it in impenetrable Fourth Amendment protection. As Part III.A demonstrates, the fact that a suspect has locked an item and made it difficult for the police to acquire the evidence does not immunize it from police authority to search. As detailed in Part III.B, lower courts have granted law enforcement considerable leeway to break into containers when searching incident to arrest. Whether the search involves a locked glove box, a locked briefcase, or a sealed container, police generally are permitted to pick the lock or even break it to conduct a search incident to arrest. Under this rule, therefore, police should be free to tinker with passwords to search the contents of a cell phone incident to arrest. However, this authority is not without limits: A crucial part of the search-incident-to-arrest doctrine requires the search to be contemporaneous with the arrest. As Part III.C explains, court decisions are very inconsistent when it comes to how long after arrest police may continue to conduct a search incident to arrest. Nevertheless, Part III.C outlines the parameters of how long police likely have to attempt to crack a cell-phone password.

A. *PASSWORD PROTECTING A PHONE DOES NOT CLOAK IT IN  
IMPENETRABLE FOURTH AMENDMENT PROTECTION  
AND PREVENT ALL WARRANTLESS SEARCHES*

If a cell-phone user has protected her phone with a strong password that combines letters, numbers, and symbols, the chances of police randomly guessing the password should be slim. With such low odds of success, our first instinct might be that the Fourth Amendment offers rigorous protection and prevents any police attempt to bypass a password without first procuring a search warrant. That assumption is incorrect. Fourth Amendment protection is not awarded on a statistical basis simply because the odds of police actually finding the evidence are low.<sup>115</sup>

Consider the following case highlighted by Professor Orin Kerr in an article about cyberspace encryption.<sup>116</sup> In *United States v. Scott*, the defendant shredded incriminating documents and threw them out with his trash.<sup>117</sup> Government agents went through Scott's trash, "painstakingly" pieced the documents back together over multiple days, and used the evidence against

---

115. Professor Orin Kerr offers the example of a burglar stealing from an unoccupied home. The burglar may correctly believe that the odds of law enforcement finding him in the house are very low. Yet, despite the statistical probability, courts still do not conclude that the burglar has a reasonable expectation of privacy in the house. Rather, because Fourth Amendment analysis is conducted from a rights-based perspective, rather than a statistical perspective, courts conclude that the burglar has no reasonable expectation of privacy in his victim's house. See Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 518 (2001).

116. *Id.* at 513-18. The discussion of the cases that follows is drawn primarily from Professor Kerr's excellent article.

117. 975 F.2d 927, 928 (1st Cir. 1992).

him.<sup>118</sup> Although individuals ordinarily do not have an expectation of privacy in trash they discard at the curb (and thus are not entitled to any Fourth Amendment protection whatsoever), Scott contended that by shredding the documents so thoroughly, he made it very difficult for the police to see any evidence and, thus, created a reasonable expectation of privacy in his shredded documents.<sup>119</sup> The First Circuit rejected this argument, explaining that while Scott went to great lengths to make it more difficult for the police to view the evidence, this did not create a privacy expectation in the trash where none existed before.<sup>120</sup> The court emphasized that a defendant's constitutional protection does not turn on the odds of recovering the evidence.<sup>121</sup>

In the cell-phone context, unlike the trash in *Scott*, individuals obviously have a reasonable expectation of privacy in the contents of their phones.<sup>122</sup> But courts have repeatedly held that the privacy interest in a phone can be overcome under the search-incident-to-arrest doctrine. Password protecting the phone, and thus making it harder for law enforcement to access the evidence, does not eliminate police authority to conduct the search incident to arrest.<sup>123</sup> Put simply, the fact that it is difficult for police to unearth

---

118. *Id.*

119. *See id.* at 928–30.

120. *See id.* at 930 (“Should the mere use of more sophisticated ‘higher’ technology in attempting destruction of the pieces of paper grant higher constitutional protection to this failed attempt at secrecy? We think not. . . . A person who prepares incriminatory documents in a secret code [or for that matter in some obscure foreign language], and thereafter blithely discards them as trash, relying on the premise or hope that they will not be deciphered [or translated] by the authorities could well be in for an unpleasant surprise if his code is ‘broken’ by the police [or a translator is found for the abstruse language], but he cannot make a valid claim that his subjective expectation in keeping the contents private by use of the secret code [or language] was reasonable in a constitutional sense.”).

121. *Id.* Courts have similarly held that drug couriers cannot claim a reasonable expectation of privacy in the drugs they are smuggling simply because they have hidden the drugs well and made it hard for law enforcement to find them. *See United States v. Sarda-Villa*, 760 F.2d 1232, 1236–37 (11th Cir. 1985) (“Drug smugglers can not assert standing solely on the basis that they hid the drugs well and hoped no one would find them.”). Likewise, courts have held that encoding communications in a foreign language or burying files deep in a computer does not add any privacy expectation. *See United States v. Longoria*, 177 F.3d 1179, 1183 (10th Cir. 1999) (speaking in foreign language); *Commonwealth v. Copenhefer*, 587 A.2d 1353, 1355–56 (Pa. 1991) (attempting to delete computer files), *abrogated on other grounds by Commonwealth v. Rizzuto*, 777 A.2d 1069 (Pa. 2001), *abrogated by Commonwealth v. Freeman*, 827 A.2d 385 (Pa. 2003).

122. *See, e.g., United States v. Finley*, 477 F.3d 250, 258–59 (5th Cir. 2007) (finding that Finley had a reasonable expectation of privacy in his cell phone even though his employer provided it to him).

123. *See Kerr, supra* note 115, at 522 (“[T]he lock is not critical to establish Fourth Amendment protection [in a briefcase]: if I have a right to keep people from looking in my briefcase . . . I will have a ‘reasonable expectation of privacy’ even without the lock.”).

evidence from a password-protected cell phone does not give the phone unlimited Fourth Amendment protection against searches.<sup>124</sup>

Of course, I do not want to suggest that password protecting the phone is completely irrelevant to Fourth Amendment analysis. When searching a cell phone that is not password protected, police essentially search a closed container, like a glove compartment in a vehicle.<sup>125</sup> When the cell phone is password protected, however, the container is not only closed, but is locked, like a glove compartment that cannot be opened without a key. The important question is therefore not whether the password somehow immunizes the phone from police investigation (it doesn't), but whether the police are permitted to open a locked container under the search-incident-to-arrest doctrine. As explained in Part III.B below, caselaw strongly suggests that police are free to attempt to unlock a password-protected cell phone.

B. *POLICE CAN SEARCH LOCKED CONTAINERS INCIDENT TO ARREST*

Although the search-incident-to-arrest doctrine has existed for over seventy years, the Supreme Court has never clearly stated whether police are permitted to open locked containers when searching incident to arrest. Nevertheless, the Court's decision in *New York v. Belton* (authorizing the search of the passenger compartment of a vehicle) broadly stated that police can search "any" container, whether "open or closed."<sup>126</sup> And the *Belton* dissenters clearly expressed their belief that the decision extended to locked containers.<sup>127</sup> As explained below, in the years since *Belton*, lower courts have reached fairly uniform consensus permitting police to search locked containers as long as they do not irreparably damage them.

---

124. See *id.* at 517 ("When the government obtains ciphertext that can only be decrypted with an individual's private key, that individual enjoys an excellent chance that the government will be unable to discover the key and decrypt the communication. However, the Fourth Amendment does not protect the individual if the government decides to devote its resources to decrypting the communication and manages to succeed.").

125. For a discussion of cell phones being treated as closed containers, see *supra* notes 72–74 and accompanying text.

126. 453 U.S. 454, 460–61 (1981) ("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. 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 . . ." (footnote omitted) (citations omitted)).

127. *Id.* at 468 (Brennan, J., dissenting) ("Under the approach taken today, the result would presumably be the same . . . if [the] search had extended to locked luggage or other inaccessible containers located in the back seat of the car."); *id.* at 472 (White, J., dissenting) ("The Court now holds that as incident to the arrest of the driver or any other person in an automobile, the interior of the car and any container found therein, whether locked or not, may be not only seized but also searched even absent probable cause to believe that contraband or evidence of crime will be found.").

### 1. Searching Locked Physical Containers

The most common example of police searching a locked container is the search of vehicles' glove compartments. For nearly three decades, courts have almost unanimously<sup>128</sup> held that police may open locked glove compartments during searches incident to arrest.<sup>129</sup>

Some courts have gone beyond glove compartments to permit searches incident to arrest of even more secure containers, such as locked safes and footlockers. In *United States v. Thomas*, the Sixth Circuit approved the search incident to arrest of a locked twenty-pound safe found inside a tote bag on the backseat of the arrestee's pickup truck.<sup>130</sup> Officers removed the car keys from the truck's ignition and found the key to the safe on the key ring. The

128. To be sure, there is contrary authority. Nearly twenty-five years ago, the Washington Supreme Court looked to its state constitution to offer a more protective holding forbidding searches of locked containers incident to arrest. *State v. Stroud*, 720 P.2d 436, 441 (Wash. 1986) (en banc) (holding that "if the officers encounter a locked container or locked glove compartment, they may not unlock and search either container without obtaining a warrant"), *overruled in part by* *State v. Valdez*, 224 P.3d 751 (Wash. 2009) (en banc); *see also id.* at 439 ("Our divergence from the decisions of federal courts is based on this heightened protection of privacy required by our state constitution."). The court offered two rationales for this divergence. First, "by locking the container, the individual has shown that he or she reasonably expects the contents to remain private." *Id.* at 441. Second, the court believed that an arrestee would be unable to retrieve a weapon or destroy evidence from a locked container, thus eliminating the primary justifications for searching incident to arrest. *See id.* The first explanation makes little sense. The search-incident-to-arrest doctrine allows searches of areas the individual expects to keep private. Police are permitted to search jacket pockets, purses, and under vehicle seats to look for weapons even though individuals have an expectation of privacy in all of those locations. The second argument is more compelling because, realistically speaking, arrestees are very unlikely to be able to escape custody, unlock a glove box, and retrieve a weapon before being stopped by police. Nevertheless, as the Washington Supreme Court acknowledged, this approach ignores the bright-line approach the U.S. Supreme Court has long embraced for searches incident to arrest.

129. *United States v. Nichols*, 512 F.3d 789, 797–98 (6th Cir. 2008) ("We therefore join the unanimous view of our sister circuits in holding that the search-incident-to-arrest authority permits an officer to search a glove box, whether open or closed, locked or unlocked."); *United States v. Gonzalez*, 71 F.3d 819, 827 (11th Cir. 1996); *United States v. Woody*, 55 F.3d 1257, 1270 (7th Cir. 1995); *United States v. McCrady*, 774 F.2d 868, 872 (8th Cir. 1985); *State v. Hanna*, 839 P.2d 450, 452 (Ariz. 1992); *People v. Perez*, 214 P.3d 502, 506 (Colo. App. 2009), *rev'd en banc*, 231 P.3d 957 (Colo. 2010); *State v. Farr*, 587 A.2d 1047, 1050 (Conn. App. Ct. 1991); *State v. Church*, No. 08006784, 2008 WL 4947653 (Del. Super. Ct. Nov. 19, 2008); *Lewis v. United States*, 632 A.2d 383 (D.C. 1993); *Staten v. United States*, 562 A.2d 90 (D.C. 1989); *Smith v. United States*, 435 A.2d 1066 (D.C. 1981) (per curiam); *State v. Gonzalez*, 507 So. 2d 772 (Fla. Dist. Ct. App. 1987); *People v. Dieppa*, 830 N.E.2d 870 (Ill. App. Ct. 2005); *Hamel v. State*, 943 A.2d 686 (Md. Ct. Spec. App. 2008); *State v. Brooks*, 446 S.E.2d 579, 588 (N.C. 1994); *State v. Massenburg*, 310 S.E.2d 619, 622 (N.C. Ct. App. 1984); *State v. Reed*, 634 S.W.2d 665 (Tenn. Crim. App. 1982); *State v. Fry*, 388 N.W.2d 565 (Wis. 1986), *overruled by* *State v. Dearborn*, 2010 WI 84, 327 Wis. 2d 252, 786 N.W.2d 97, *petition for cert. filed*, No. 10-7057 (U.S. Oct. 13, 2010). In many cases, officers unlocked the glove box by simply using the ignition key. In some cases however, courts have upheld searches where police physically forced open the glove box without a key. *See, e.g., Smith*, 435 A.2d at 1068.

130. 11 F.3d 620, 625, 628 (6th Cir. 1993).

court concluded that searching the safe fell squarely within the search-incident-to-arrest doctrine.<sup>131</sup> Similarly, an Illinois court upheld the search incident to arrest of a locked footlocker on the grounds that it was no different than a locked glove compartment.<sup>132</sup>

Courts have likewise permitted police to search locked briefcases<sup>133</sup> and overnight bags<sup>134</sup> incident to arrest. One federal court even upheld a search incident to arrest when police pried open the latch of a locked briefcase with a screwdriver.<sup>135</sup> Lower courts have also upheld police searches of sealed boxes in which police had to tear through tape to access the contents. For instance, a Florida appellate court approved the search incident to arrest of “two large, sealed U-Haul boxes” in the backseat of a station wagon.<sup>136</sup> Without extensive analysis, the Fifth Circuit upheld a similar search incident to arrest of “cardboard boxes sealed with masking tape.”<sup>137</sup>

Courts have been less consistent in cases where police tamper with the structural integrity of the passenger compartment of the vehicle. As a general rule, courts have forbidden police from dismantling the interior of the vehicle when searching incident to arrest.<sup>138</sup> Thus, courts have suppressed evidence police found where police removed a vehicle seat<sup>139</sup> or dismantled a tailgate<sup>140</sup> when searching incident to arrest. Yet even in the face of this logical rule,<sup>141</sup> a number of lower courts have given police leeway to conduct searches of sealed areas incident to arrest. For example, the Eighth Circuit upheld a search incident to arrest of the space between the window’s rubber seal and the door panel.<sup>142</sup> A federal court in

---

131. *See id.* at 628.

132. *People v. Tripp*, 715 N.E.2d 689, 698 (Ill. App. Ct. 1999).

133. *See United States v. Valiant*, 873 F.2d 205, 206 (8th Cir. 1989); *United States v. Howe*, 313 F. Supp. 2d 1178, 1184–86 (D. Utah 2003).

134. *See Pack v. Commonwealth*, 368 S.E.2d 921, 922 (Va. Ct. App. 1988).

135. *See Howe*, 313 F. Supp. 2d at 1182, 1184–85.

136. *Shaw v. State*, 449 So. 2d 976, 978 (Fla. Dist. Ct. App. 1984).

137. *United States v. Alvarado Garcia*, 781 F.2d 422, 424 (5th Cir. 1986), *overruled on other grounds by United States v. Bengivenga*, 845 F.2d 593 (5th Cir. 1988).

138. *See* 1 DAVID S. RUDSTEIN ET AL., CRIMINAL CONSTITUTIONAL LAW § 2.06[4][b], at 2-240 (2009) (“[L]ower courts [have] generally excluded areas that required dismantling, such as the interior of the door panels or the tailgate, the upholstery of the car, the area under the floorboards, or the area behind the glove compartment or radio.” (footnotes omitted)).

139. *State v. Cuellar*, 511 A.2d 745, 748 (N.J. Super. Ct. Law Div.) (rejecting search incident to arrest where “[t]he police officer then removed the seat entirely from the automobile, which exposed the entire panel, and pulled away the panel for the chassis”), *aff’d*, 523 A.2d 662 (N.J. Super. Ct. App. Div. 1986).

140. *See United States v. Patterson*, 65 F.3d 68, 71 (7th Cir. 1995).

141. *See* David S. Rudstein, *The Search of an Automobile Incident to an Arrest: An Analysis of New York v. Belton*, 67 MARQ. L. REV. 205, 239–40 (1984) (arguing that police should not be permitted to dismantle parts of vehicles during searches incident to arrest).

142. *United States v. Barnes*, 374 F.3d 601, 604 (8th Cir. 2004) (“The search incident to arrest in this case involved the area immediately inside the rubber window seal . . .”).

Massachusetts approved the search of a heating vent inside of the passenger compartment of a vehicle.<sup>143</sup> The Seventh Circuit allowed police to dislodge a removable radio and search the space in the dashboard where it had been located.<sup>144</sup> Several courts have upheld searches of the area beneath a gearshift incident to arrest, even where officers had to loosen the plastic cover and snap out the console to gain access.<sup>145</sup>

Although it is difficult to state a rule that explains the results of all of these cases, when assessing the search incident to arrest of locked or sealed containers, three key principles emerge. First, courts almost always permit police to utilize a key to unlock containers. Second, when no key is available, some courts approve of police physically breaking locks to examine the container's contents, although these courts have not offered detailed analysis justifying their decisions. Finally, when dealing with sections of the passenger compartment of a vehicle that are easily disassembled (such as gear shift covers or removable radios), courts seemingly embrace a version of the slogan "you break it, you buy it," and uphold the searches as long as officers do not damage the vehicle. It is only when police have broken items or dismantled major sections of a vehicle that courts unequivocally reject the search-incident-to-arrest doctrine.

## 2. Searching a Locked (Password-Protected) Phone Is Permissible

To date, only two courts have been called on to determine whether individuals can be forced to turn over passwords to their computer files, and both cases involved grand-jury subpoenas, rather than searches incident to arrest.<sup>146</sup> Nevertheless, cases involving searches incident to arrest of password-protected phones are likely to arise in the near future. The number of Americans utilizing iPhones and other smart phones is growing exponentially each year, and each new generation of smart phone is capable of holding more and more private data.<sup>147</sup> Either out of fear of law enforcement or the simple possibility of losing the phone, users are likely to

---

143. *United States v. Patrick*, 3 F. Supp. 2d 95, 99 (D. Mass. 1998) (noting that the First Circuit permits searches of any area in passenger compartment as long as officers do not "dismantl[e] door panels or other parts of the car" (internal quotation mark omitted)), *aff'd*, 248 F.3d 11 (1st Cir. 2001). The *Patrick* court found that the search occurred too long after the arrest to be a contemporaneous search incident to arrest, but it ultimately upheld the search under the automobile exception. *See id.* at 104.

144. *United States v. Willis*, 37 F.3d 313 (7th Cir. 1994); *see also* *United States v. Veras*, 51 F.3d 1365, 1368 (7th Cir. 1995) (upholding search of secret compartment "[b]uilt into the deck between the back seat and the rear window" under the search-incident-to-arrest doctrine).

145. *State v. Homolka*, 953 P.2d 612 (Idaho 1998); *People v. Eaton*, 617 N.W.2d 363 (Mich. Ct. App. 2000).

146. *See* *United States v. Kirschner*, Misc No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

147. *See* Shan Li, *iPhone 4 Deliveries Beat Official Launch*, L.A. TIMES, June 23, 2010, at B3.

begin password protecting their phones at greater rates.<sup>148</sup> Indeed, there are already a handful of cases where police have encountered password-protected phones and either procured the password by consent<sup>149</sup> or given up on searching the phone because of the password.<sup>150</sup> As password protection becomes more common, police officers who believe a phone contains incriminating evidence, and who lack the necessary suspicion or time to get a warrant, will try to crack passwords and gain access to cell phones.

It seems clear that police can attempt to crack a cell-phone password during a search incident to arrest.<sup>151</sup> Just as police are permitted to try all of the keys on the defendant's keychain until they locate the one that unlocks the glove compartment, police should be able to try multiple different combinations in an effort to discover the password to a phone.

Of course, there should still be limits on the manner in which police can search a cell phone incident to arrest. First, as with tangible objects like an automobile, police should be cabined by a rule forbidding them from destroying an object to search it incident to arrest. Many cell phones contain a function that deletes the contents of the phone if the password is incorrectly entered a certain number of consecutive times. If the phone alerted the officer that another incorrect password entry would erase the contents of the phone, police should not be permitted to make that final guess.<sup>152</sup>

A second restriction on police efforts to break a password is the requirement that the search of the phone be contemporaneous with arrest. Breaking the password may be time-consuming, and for a search to be truly incident to arrest, there must be time limits on how long police can take to conduct the search. Part III.C discusses the major unresolved issues related to the temporal limit on searching cell phones incident to arrest.

### C. ATTEMPTS TO BREAK PASSWORDS MUST BE CONTEMPORANEOUS WITH ARREST

In remarking on the breadth of the search-incident-to-arrest doctrine, Professor Wayne Logan explained in 2001 that, “[i]ncreasingly, the sole

---

148. See *United States v. Lasalle*, Cr. No. 07-00032 SOM, 2007 WL 1390820, at \*2 (D. Haw. May 9, 2007) (noting that police found two phones during a drug arrest, one of which was password-protected).

149. See *People v. Villasana*, No. F056773, 2010 WL 7122, at \*3 (Cal. Ct. App. Jan. 4, 2010) (upholding search of phone that had been password-protected).

150. See *People v. Hall*, No. D053791, 2009 WL 4549188, at \*2 (Cal. Ct. App. Dec. 7, 2009).

151. See *supra* Part III.B.1.

152. Just as police are not permitted to tear apart a vehicle's upholstery in searching incident to arrest, they should not be permitted to destroy the contents of a cell phone to recover evidence. Of course, if the failed password attempts actually resulted in wiping the phone's contents clean, there would be no evidence for the police to acquire through the search incident to arrest of the phone.

limit[] on search incident authority [is] that the search be more or less ‘contemporaneous’ with the arrest.”<sup>153</sup> Nearly a decade later, Professor Logan’s observation rings true for the search incident to arrest of cell phones. Unfortunately, the meaning of contemporaneous varies widely from court to court. Some find searches occurring hours after arrest contemporaneous, whereas others believe even twenty minutes is far too long. Further complicating the contemporaneousness inquiry is that the length of time police have to crack a password may depend on whether cell phones are categorized as an “item associated with the person of an arrestee,” or as property near the arrestee. If cell phones are items associated with the person of an arrestee, a 1974 Supreme Court case seemingly gives police great flexibility to search them long after arrest, even after they have been brought to the police station.<sup>154</sup> By contrast, if cell phones are possessions near the arrestee, a 1977 Supreme Court decision limits searches to a short time after arrest, and primarily to the scene of the arrest itself.<sup>155</sup>

#### 1. Different Rules for Searching Items Associated with the Person and Items That Are Merely Nearby Possessions

In ascertaining how long police can spend trying to crack a password, it is best to begin by determining whether cell phones are items immediately associated with the arrestee or are merely possessions near the arrestee. This distinction requires us to parse two Supreme Court cases from the 1970s.

In the somewhat obscure case of *Edwards*, police arrested Edwards at 11 p.m. for attempting to break into a government building.<sup>156</sup> Edwards was promptly brought to jail, processed, and placed in a cell.<sup>157</sup> Overnight, police discovered that the perpetrator had attempted to enter a wooden window and that he would likely have paint chips from the window on his clothing.<sup>158</sup> The following morning, ten hours after his arrest, police took Edwards’s clothing from him to search for paint chips.<sup>159</sup> Edwards moved to suppress the evidence on the grounds that the search of his clothes occurred too long after arrest to fall within the search-incident-to-arrest exception.<sup>160</sup> The Supreme Court rejected Edwards’s argument and gave police wide

---

153. Wayne A. Logan, *An Exception Swallows a Rule: Police Authority To Search Incident to Arrest*, 19 YALE L. & POL’Y REV. 381, 396 (2001).

154. See *United States v. Edwards*, 415 U.S. 800, 805 (1974).

155. See *United States v. Chadwick*, 433 U.S. 1, 15 (1977).

156. 415 U.S. at 801.

157. *Id.*

158. *Id.* at 801–02.

159. *Id.* at 802.

160. See *id.*

authority to conduct the search incident to arrest well after the arrest was conducted.<sup>161</sup>

Three years later, in the better-known case of *Chadwick*, officers arrested Chadwick as he attempted to load a double-locked footlocker into his vehicle.<sup>162</sup> One set of agents brought Chadwick to a federal building, and another group of agents followed behind with the footlocker.<sup>163</sup> Approximately ninety minutes after the arrest, federal agents opened the footlocker and discovered a large quantity of marijuana.<sup>164</sup> Unlike in *Edwards*, the Supreme Court rejected the Government's argument that the footlocker could be searched incident to arrest. In a brief footnote, the Court distinguished *Edwards* by explaining that "[u]nlike searches of the person, searches of possessions within an arrestee's immediate control cannot be justified by any reduced expectations of privacy caused by the arrest."<sup>165</sup> The Court further explained:

Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.<sup>166</sup>

The Court's decisions in *Edwards* and *Chadwick* thus offer two different rules for the temporal scope of searches incident to arrest. If the search is of items associated with the person, police have great flexibility and can conduct the search many hours after arrest. If, however, the police search possessions that are not associated with the person and are merely nearby, then there is a more rigid time limitation. In the three and a half decades since the *Edwards* and *Chadwick* decisions, the Supreme Court has offered no additional guidance on this distinction. There are, however, a few relatively clear, decipherable principles from lower court decisions.

Lower courts have repeatedly concluded that, in addition to clothing, police may search an arrestee's wallet incident to arrest at the station house because a wallet conceptually falls under *Edwards* as an item typically found on the person of an arrestee and thus closer to clothing than, for example, the footlocker in *Chadwick*.<sup>167</sup> Similarly, courts have upheld station house

---

161. See *id.* at 805–09.

162. See *United States v. Chadwick*, 433 U.S. 1, 4 (1977).

163. *Id.*

164. *Id.* at 5.

165. *Id.* at 16 n.10 (citations omitted).

166. *Id.* at 15.

167. See *United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993) (allowing search of wallet and the address book inside of it at the station house and citing *Edwards*); *United States v. McEachern*, 675 F.2d 618, 622 (4th Cir. 1982) (approving search incident to arrest of wallet at police station); *United States v. Baldwin*, 644 F.2d 381, 384 (5th Cir. 1981) (upholding search

searches incident to arrest of purses,<sup>168</sup> duffle bags,<sup>169</sup> and backpacks<sup>170</sup> because they more closely resemble items on the person rather than nearby possessions. As Professor Wayne LaFare observed in his influential treatise, courts have “rather consistently” held that under *Edwards* police can search

---

incident to arrest at station house of wallet “a few hours” after arrest under *Edwards*); *United States v. Passaro*, 624 F.2d 938, 944 (9th Cir. 1980) (upholding search of wallet at police station under *Edwards* because a wallet is much closer to a person than a footlocker or a briefcase); *United States v. Castro*, 596 F.2d 674, 677 (5th Cir. 1979) (relying on *Edwards* to permit police to read papers in wallet during station house search); *Chambers v. State*, 422 N.E.2d 1198, 1203 (Ind. 1981) (upholding search incident to arrest of wallet at station because it “was immediately associated with the person of appellant” and thus cannot fall under *Chadwick*); *People v. Knight*, 333 N.W.2d 94, 95, 98 (Mich. Ct. App. 1983) (upholding search of defendant’s wallet incident to arrest at police station, though conducting no analysis of the issue); *State v. Rodewald*, 376 N.W.2d 416, 419 (Minn. 1985) (“A wallet is not akin to the container in *Chadwick* since it is immediately associated with the person of the arrestee.”); *People v. Blankmsee*, 764 N.Y.S.2d 331, 334 (Sup. Ct. 2003) (concluding without analysis that drugs found in defendant’s wallet during search at precinct station was permissible under search-incident-to-arrest doctrine); *State v. Garcia*, 665 P.2d 1381, 1382–83 (Wash. Ct. App. 1983) (upholding search incident to arrest of wallet at station house); *Roose v. State*, 759 P.2d 478, 484 (Wyo. 1988) (upholding search of wallet while defendant was being held in detention at a hospital, under *Edwards*).

168. See, e.g., *United States v. Venizelos*, 495 F. Supp. 1277, 1283 (S.D.N.Y. 1980) (“[A handbag was property immediately associated with the person because it was small and within the arrestee’s grasp and because] [i]t carried items normally closely associated with the person itself [including] identification, cosmetics, money, a wallet, and other items one would normally carry at all times. Indeed, it is reasonable to suppose that had it not been seized at the time of the arrest, the defendant probably would have brought the handbag with her to the DEA district office for identification and to assist in ‘booking . . .’”); *People v. Harris*, 164 Cal. Rptr. 296 (Ct. App. 1980) (authorizing station house search of purse and wallet contained therein because California law considers a purse to be a normal extension of the person); *People v. Thomas*, 760 N.E.2d 1012 (Ill. App. Ct. 2001) (finding search at police station to be consistent with *Edwards*); *People v. Mannozi*, 632 N.E.2d 627, 632 (Ill. App. Ct. 1994) (“[A] purse, unlike a footlocker, has been held to be an item immediately associated with the person of an arrestee, because it is carried on the person at all times.”); *Preston v. State*, 784 A.2d 601, 608 (Md. Ct. Spec. App. 2001) (rejecting delayed search of automobile but recognizing that courts considering the question have generally concluded that a purse, like a wallet, is an object “immediately associated with the person”); *State v. Greene*, 785 S.W.2d 574, 577 (Mo. Ct. App. 1990) (upholding station house search of purse because “a woman’s purse is, like the arrestee’s clothes in *Edwards*, more immediately associated with the person of the accused than is other personal property, such as luggage or an attache case” (internal quotation mark omitted)); *State v. Woods*, 637 S.W.2d 113, 116 (Mo. Ct. App. 1982) (same); *State v. Wade*, 573 N.W.2d 228 (Wis. Ct. App. 1997) (relying on *Edwards* to authorize search incident to arrest of purse at police station).

169. See *United States v. Morales*, 549 F. Supp. 217, 224 & n.5 (S.D.N.Y. 1982) (concluding without explanation that a duffle bag was immediately associated with the person and that it could be searched after arrest at the police headquarters).

170. See *People v. Boff*, 766 P.2d 646, 651 n.9 (Colo. 1988) (en banc) (offering detailed analysis of *Edwards* and *Chadwick* and concluding that backpack could be searched at station incident to arrest because it “is more like a purse than a two-hundred pound double-locked footlocker”); *id.* at 651 (“A search at the police station of a suspect, his clothes, and personal property immediately associated with his person, is justified to the same extent that such a search could have been made at the time and place of arrest.”).

incident to arrest the “pockets, wallet, [and] other containers on the person” at the station house following arrest.<sup>171</sup> To the extent conflicting authority finds items as possessions falling under *Chadwick*, the cases typically involve purses and briefcases found in the arrestee’s vehicle or otherwise not attached to the arrestee’s body.<sup>172</sup>

As explained in Part III.C.2 below, the fact that wallets, purses, and other items on the arrestee are almost universally considered part of the person, and are thus searchable incident to arrest hours later at the station house, strongly suggests that cell phones stored on an arrestee should fall into this category as well.

## 2. Cell Phones Will Often Be Items Associated with the Person, Giving Police a Lengthy Time To Search

To determine how long police can spend trying to crack a cell-phone password, courts must first decide whether the phone falls under *Edwards* or *Chadwick*. Most courts deciding searches incident to arrest of cell phones have not addressed this question, and those that have undertaken the task have reached conflicting results.

A few courts have held that cell phones constitute possessions associated with the person of an arrestee under *Edwards*, and that law-enforcement officers have flexibility in the time it takes them to search the phones incident to arrest. Once again, the key case supporting this approach is the Fifth Circuit’s decision in *United States v. Finley*.<sup>173</sup> In *Finley*, police arrested the defendant at a traffic stop and then transported him to a coconspirator’s house where the police were executing a search.<sup>174</sup> At this new location, DEA agents searched Finley’s cell phone and found evidence linking him to a drug conspiracy.<sup>175</sup> Citing *Edwards*, the *Finley* court rejected the argument that the search of Finley’s cell phone was too far removed from his arrest.<sup>176</sup> The court specifically held that Finley’s phone should not fall into the

171. See LAFAVE, *supra* note 18, § 5.3(a), at 146 (footnotes omitted) (citing numerous cases).

172. See, e.g., *United States v. Monclavo-Cruz*, 662 F.2d 1285, 1286 (9th Cir. 1981) (rejecting search incident to arrest of purse at the stationhouse an hour after arrest when purse was “either in her hand, on her lap, or on the seat of the car at the time of arrest”); *United States v. Calandrella*, 605 F.2d 236, 247–50 (6th Cir. 1979) (concluding briefcase was an item within the arrestee’s immediate control and could not be searched later at the station under *Edwards*); *United States v. Schleis*, 582 F.2d 1166, 1170–72 (8th Cir. 1978) (same), *overruled by* *United States v. Morales*, 923 F.2d 621 (8th Cir. 1991); *Kuhn v. State*, 439 So. 2d 291, 295 (Fla. Dist. Ct. App. 1983) (rejecting station house search incident to arrest of briefcase found in arrestee’s truck); *State v. Bushberger*, No. 95-1140-CR, 1995 WL 581122, at \*3 (Wis. Ct. App. Oct. 4, 1995) (concluding that briefcase found in backseat of vehicle could not be searched incident to arrest at the station).

173. 477 F.3d 250, 258–60 (5th Cir. 2007).

174. *Id.* at 253.

175. *Id.* at 254–55.

176. *Id.* at 260 n.7.

*Chadwick* category of property not immediately associated with the person of an arrestee because the cell phone “was on his person at the time of his arrest.”<sup>177</sup> A handful of additional cases have reached the same conclusion and upheld searches of cell phones at a police station under the *Edwards* doctrine.<sup>178</sup>

By contrast, the *Park* court concluded that cell phones fell under *Chadwick*, and rejected a search conducted ninety minutes after arrest at the police station. It concluded that cell phones “should be considered ‘possessions within an arrestee’s immediate control’ and not part of ‘the person,’”<sup>179</sup> ultimately explaining:

[C]ellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.<sup>180</sup>

Thus, the court concluded that the search of *Park*’s cell phone at the station house ninety minutes after arrest could not be justified under the search-incident-to-arrest doctrine.<sup>181</sup>

177. *Id.*

178. *United States v. Murphy*, 552 F.3d 405, 412 (4th Cir. 2009); *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*] exception[] to the Fourth Amendment’s reasonableness requirements.”); *United States v. Curry*, Criminal No. 07-100-P-H, 2008 WL 219966, at \*10 (D. Me. Jan. 23, 2008); *United States v. Diaz*, No. CR 05-0167 WHA, 2006 WL 3193770, at \*4 (N.D. Cal. Nov. 2, 2006); *People v. Diaz*, 81 Cal. Rptr. 3d 215, 217–18 (Ct. App. 2008); *see also United States v. Lynch*, 908 F. Supp. 284, 289 (D.V.I. 1995) (relying on *Edwards* and concluding that a pager was immediately associated with the arrestee). A number of other courts have upheld searches at the station house, although with no discussion of the *Chadwick-Edwards* distinction. *See Brady v. Gonzalez*, No. 08 C 5916, 2009 WL 1952774, at \*2 (N.D. Ill. July 2, 2009); *United States v. Brookes*, No. CRIM 2004-0154, 2005 WL 1940124, at \*1 (D.V.I. June 16, 2005); *United States v. Cote*, No. 03CR271, 2005 WL 1323343, at \*6 (N.D. Ill. May 26, 2005).

179. *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573, at \*8 (N.D. Cal. May 23, 2007) (quoting *United States v. Chadwick*, 433 U.S. 1, 16 n.10 (1977)).

180. *Id.* (footnote omitted).

181. *See id.* at \*9. In the only other case to adopt the *Park* court’s reasoning, prosecutors conceded that a seized cell phone was not an element of the defendant’s clothing when it was seized. *See United States v. Lasalle*, Cr. No. 07-00032, 2007 WL 1390820 (D. Haw. May 9, 2007). In *Lasalle*, agents searched *Lasalle*’s cell phone at the DEA office “somewhere between two hours and fifteen minutes to three hours and forty-five minutes” after his arrest. *Id.* at \*7. The court concluded that “[g]iven the time period and physical distance between the arrest and search, the search was not ‘at about the same time of the arrest’ or ‘roughly contemporaneous’ with the arrest.” *Id.*; *see also United States v. Wall*, No. 08-60016-CR, 2008

In the battle between the *Finley* line of reasoning that cell phones are associated with the person of the arrestee and the *Park* view that phones are nearby possessions, the *Park* court appears to have the weaker argument. First, and quite bizarrely, the *Park* court concluded that the cell phone could not be associated with the person of an arrestee even though police physically removed it from his person at booking.<sup>182</sup> As detailed above, courts have repeatedly held that wallets found in arrestees' pockets (as well as purses and backpacks on an arrestee) should be considered items associated with the person of the arrestee, which can be searched at the station house under *Edwards*.<sup>183</sup> When police find a cell phone in an arrestee's pocket, precedent therefore strongly suggests it should be searchable at the station house.

Second, the *Park* court took the position that cell phones are possessions within the arrestee's immediate control because they contain a wealth of private information. However, the court offered no explanation as to why the quantity of information held in a phone had anything to do with whether it was associated with an arrestee's person or was merely a nearby possession. If storing a large quantity of information precludes an item from being associated with the person of an arrestee, then arguably the clothing in *Edwards* should not have qualified for such a designation. After all, *Edwards*'s clothing revealed that he had been at the crime scene and modern technology could provide detailed analysis linking fiber samples to the crime. Or consider the enormous amount of information police can obtain from searching a wallet—generally held to be associated with the person of an arrestee—including where the arrestee banks (via his ATM card); where he shops (via his rewards cards); whether he has any medical conditions (via medical cards); pictures of his children; and more scandalous information such as motel key cards, condoms, or the phone number of his mistress. These items do not cease to be on the person of an arrestee simply because they convey a wealth of information.

Moreover, the idea that an electronic container cannot be associated with the person of an arrestee is inconsistent with the use of cell phones in everyday life. Many people exercise with an MP3 player (including iPhones) securely strapped to their biceps.<sup>184</sup> It is difficult to comprehend how a cell phone that is literally attached to an arrestee's arm could not be associated

---

WL 5381412, at \*3 (S.D. Fla. Dec. 22, 2008) (rejecting a search of a cell phone at a police station because "it was not contemporaneous with the arrest," although not discussing *Edwards* or *Chadwick*), *aff'd*, 343 F. App'x 564 (11th Cir. 2009) (per curiam).

182. 2007 WL 1521573, at \*2.

183. See *supra* notes 167–70 and accompanying text.

184. For one of the dozens of versions of this product, see *Tune Belt Sport Armband for iPhone 3GS, iPhone 4 and More*, AMAZON.COM, [http://www.amazon.com/Tune-Belt-Armband-iPhone-Blackberry/dp/B002NL2WYQ/ref=sr\\_1\\_1?s=mp3&ie=UTF8&qid=1278100000&sr=1-1](http://www.amazon.com/Tune-Belt-Armband-iPhone-Blackberry/dp/B002NL2WYQ/ref=sr_1_1?s=mp3&ie=UTF8&qid=1278100000&sr=1-1) (last visited Feb. 28, 2011).

with the person of an arrestee.<sup>185</sup> Yet, under the *Park* court's reasoning, even cell phones that are physically strapped onto an arrestee's body could never be associated with the person of the arrestee because they contain so much data.

The problem with the *Park* decision is that it embraces a bright-line rule in which all cell phones should constitute nearby possessions and can never be items associated with the arrestee's person. In some instances, such as when police find a phone in a briefcase or sitting on the front passenger seat of a vehicle, it makes sense to say a cell phone is a possession near the arrestee. In cases where the cell phone is in the arrestee's pocket, attached to his arm, or clipped to his belt, it is far less compelling to suggest that the phone is never associated with the person of an arrestee.

In short, there is no easy, all-purpose answer to the question of whether a cell phone should be considered an item associated with the person of an arrestee or merely a nearby possession. The categorization depends on the specific facts of the case. In some instances, police should be permitted to search a cell phone hours after arrest at the police station, whereas in other cases such elongated searches should be forbidden.

### 3. If Cell Phones Are Merely Possessions, How Long Can Police Spend Searching Them Before the Search Ceases To Be Contemporaneous?

It is easy to see why the *Edwards–Chadwick* issue has gathered considerable attention in the debate over searching cell phones incident to arrest.<sup>186</sup> If a cell phone is part of the person, then police should be permitted to take it to the station and conduct a warrantless search for hours after arrest. Accordingly, observers may instinctually be reluctant to place cell phones in the *Edwards* box, which gives police wide search latitude. Yet, categorizing cell phones as possessions near an arrestee that fall under *Chadwick* does not end the analysis. Police may still search such nearby items incident to arrest as long as the search is contemporaneous. If the phones fall under *Chadwick*, the key question—and the question that is too often ignored by courts in the cell-phone context—is how long police have to conduct the search. Are officers limited to five minutes after arrest, or can they take much longer? Unfortunately, there is no clear answer to this question.

---

185. It is common to hear the metaphor that people are so addicted to their cell phones that the phones are attached to them. It is possible, though, that this derogatory metaphor might one day become a reality. Although farfetched in 2011, it is plausible that in the near future a wireless device could be surgically attached to a person's forearm so that the Internet would, quite literally, always be at his fingertips. Under the *Park* court's reasoning, however, the phone would remain a nearby possession falling under *Chadwick*.

186. See Orso, *supra* note 52, at 203–06; Stillwagon, *supra* note 88, at 1192–94.

Although the Supreme Court has trumpeted the need for bright-line rules in the search-incident-to-arrest context, the Court has not adopted a bright-line rule dictating how long police can take to conduct such searches.<sup>187</sup> Not surprisingly, lower court decisions often appear to be completely inconsistent with one another. Perhaps for this reason academic commentators have failed to offer even a presumptive rule (such as the idea that searches within thirty minutes of arrest are typically contemporaneous, while longer time delays are usually impermissible)<sup>188</sup> because there are too many outlying decisions that would undercut such a presumption.<sup>189</sup>

Accordingly, police must be guided by high-level principles offering little practical guidance. The overarching concept provides simply that police must conduct a search as soon as is practicable. Courts are willing to uphold searches taking longer periods of time when there are intervening events,<sup>190</sup> like when police must wait for additional officers to secure the scene.<sup>191</sup> If the search appears to be part of a “continuous series of events,”<sup>192</sup> rather than an afterthought, courts are more likely to uphold the

---

187. Over twenty-five years ago, Professor Albert Alschuler criticized the Court for failing to create any rule as to what constitutes “contemporaneous with arrest.” See Albert W. Alschuler, *Bright Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227, 281–82 (1984) (“[T]he Court offered no basis for determining whether a search conducted thirty minutes or an hour after an arrest would remain a ‘contemporaneous incident.’ This sort of uncertainty may be more troublesome than the uncertainty inherent in a system of case-by-case adjudication . . .”). The problem persists to this day. See Logan, *supra* note 153, at 412 n.189 (citing *United States v. McLaughlin*, 170 F.3d 889, 892 (9th Cir. 1999) (“There is no fixed outer limit for the number of minutes that may pass between an arrest and a valid, warrantless search that is a contemporaneous incident of the arrest.”)).

188. Compare *United States v. Weaver*, 433 F.3d 1104, 1110 n.1 (9th Cir. 2006) (upholding search after ten- to fifteen-minute delay, though reiterating that “time alone is never dispositive of the contemporaneity inquiry”), *People v. Malloy*, 178 P.3d 1283, 1287 (Colo. App. 2008) (upholding search occurring a little over thirty minutes after arrest), and *State v. Hernandez*, 113 P.3d 437, 438 (Or. Ct. App. 2005) (upholding search occurring twenty to thirty minutes after arrest), with *United States v. \$639,558 in U.S. Currency*, 955 F.2d 712, 716–17, 716 n.7 (D.C. Cir. 1992) (rejecting search-incident-to-arrest doctrine for a search conducted between thirty and sixty-three minutes after arrest), and *United States v. Vasey*, 834 F.2d 782, 787–88 (9th Cir. 1987) (search of automobile thirty to forty-five minutes after arrest was too long to be incident to arrest).

189. See, e.g., *United States v. Hrasky*, 453 F.3d 1099 (8th Cir. 2006) (upholding search occurring more than one hour after arrest, although over vigorous dissent); *State v. Barksdale*, 540 A.2d 901, 907 (N.J. Super. Ct. App. Div. 1988) (finding search more than ten minutes after arrest to be “anything but ‘a contemporaneous incident of that arrest’”).

190. See, e.g., *United States v. Scott*, 428 F. Supp. 2d 1126, 1131 (E.D. Cal. 2006) (“Some courts consider whether the ‘arresting officers conducted the search as soon as it was practical to do so,’ or if there were any intervening acts occurring before the search, unrelated to the search.” (quoting *McLaughlin*, 170 F.3d at 892)).

191. See *State v. Ullock*, No. 93-1874-CR, 1994 WL 100324 (Wis. Ct. App. Mar. 30, 1994) (upholding search incident to arrest forty minutes after arrest because officer was alone on the scene and had good reason to wait for another individual to arrive on the scene before leaving the arrestee unsupervised).

192. *United States v. Smith*, 389 F.3d 944, 951 (9th Cir. 2004).

search. Indeed, many courts will even give police leeway to conduct a search incident to arrest after officers remove an arrestee from the scene, so long as there is a good reason for the delay and the police conduct the search expeditiously.<sup>193</sup>

While courts have refused to draw bright-line time limits on searches incident to arrest, the contours of the caselaw suggest that an outer time limit exists. It is easy to locate hundreds of (non-cell-phone) cases in which courts permitted searches incident to arrest five, ten, twenty, and even sixty minutes after arrest.<sup>194</sup> But very few cases address searches that occur more than an hour after arrest.<sup>195</sup> The absence of such cases suggests that there truly is an implicit outer limit on the time police have to conduct searches incident to arrest.

#### 4. Will Police Have Enough Time To Crack the Password?

The key remaining question is whether, practically speaking, police will be able to successfully crack a cell-phone password while complying with the time limits of the search-incident-to-arrest doctrine. The answer to this question likely turns on where the cell phone is located when the owner is arrested. If a cell phone is found on an arrestee or in his pocket it should be considered part of his person, giving police the power to bring it to the station and search it even hours after the arrest. If police discover a cell phone within the grabbing space of an arrestee, such as in a briefcase or lying on the passenger seat of an automobile, they still may search it but typically must do so at the scene and likely within minutes, or at most an hour, of the arrest. Thus, police may have a short period of time to try to crack the password of a cell phone found near an arrestee, and they may have a considerably longer period of time to crack the password of a cell phone found in an arrestee's pocket. As explained below, they will have trouble doing the former but could accomplish the latter.

If police must search a cell phone on the scene and have only a few minutes to do so, a password will likely prevent the police from accessing the phone's contents. In most cases, police simply will not be able to decipher a

---

193. Compare *McLaughlin*, 170 F.3d at 892 (upholding a search that officers began five minutes after arrestee was removed from the scene and continued for eleven minutes until the officer discovered contraband), and *United States v. Doward*, 41 F.3d 789 (1st Cir. 1994) (upholding search incident to arrest begun three minutes after individual was placed under arrest and thirty seconds after he had been driven from the scene), with *United States v. Dennison*, 410 F.3d 1203, 1209 (10th Cir. 2005) ("A search incident to arrest is unlawful when a suspect is arrested, removed from the scene, and en route to the police station when the search of the arrestee's passenger compartment begins.").

194. See V.G. Lewter, Annotation, *Modern Status of Rule as to Validity of Nonconsensual Search and Seizure Made Without Warrant After Lawful Arrest as Affected by Lapse of Time Between, or Difference in Places of, Arrest and Search*, 19 A.L.R.3d 727 (1968).

195. See, e.g., *People v. Landry*, 80 Cal. Rptr. 880, 884 (Ct. App. 1969) (rejecting search occurring one hour and fifteen minutes after arrest).

password during the commotion of an arrest. That said, it is possible that police could guess the password in some cases. One in five Americans uses an overly simplistic password such as “123456,” and an officer might simply get lucky by trying the most common passwords.<sup>196</sup> Officers also have access to an arrestee’s driver’s license, which contains his birth date and home address—both of which are commonly used as passwords. Thus, while the chance of an officer cracking the password in a short time on the scene is limited, it is possible.

In the cases where police bring the cell phone to the station house because it is considered part of the arrestee’s person in that jurisdiction, the chances of cracking the password increase dramatically, particularly for certain phones. Take the iPhone as an example. The iPhone’s password function offers three key protections: (1) a four-digit numerical code; (2) a requirement that consecutively entered incorrect passwords disable the phone for a short period before the user can try another password; and (3) the option to have the contents of the phone deleted if the incorrect password is entered ten times.<sup>197</sup> Unfortunately, these protections are extremely weak.

A four-digit numerical code provides only 10,000 combinations. While this might prevent most human guessing, it would not stop a brute-force computer program that sequentially inputs every numerical combination.<sup>198</sup> If law enforcement utilized a very simple computer program to try all 10,000 combinations in a row, they would be able to crack the password in minutes. While police stations likely do not currently have such programs at their fingertips, it is quite possible they will in the near future as technology becomes more ubiquitous.

Moreover, even if police never set up the program to crack passwords, they may be able to bypass the password altogether by hacking into the phone. One well-known computer hacker has authored a book called *iPhone Forensics*, which explains how to remove data from the phone.<sup>199</sup> The same hacker proudly advertises that he teaches courses on the topic to law-enforcement agencies, including lessons on bypassing pass codes.<sup>200</sup>

Even if police agencies lack the money or time to enroll any of their officers in computer-forensics classes, they can turn to numerous Internet

---

196. See Vance, *supra* note 12 (noting that one percent of 32 million passwords stolen by a hacker were “123456” (internal quotation marks omitted)).

197. See Jeff Richardson, *A Look at the iPhone Passcode Lock Feature*, IPHONE J.D. (Sept. 28, 2009), [http://www.iphonejd.com/iphone\\_jd/2009/09/iphone-passcode-lock.html](http://www.iphonejd.com/iphone_jd/2009/09/iphone-passcode-lock.html).

198. Joe Kissell, *Top Password Tips: Foolproof Ways To Create, Remember and Manage Passwords*, MACWORLD, Sept. 1, 2009, 2009 WLNR 26376198; Jay Sartori, *iPhone Passcode Bugs Revealed*, NETWORK WORLD, Sept. 2, 2009, 2009 WLNR 17527305.

199. See JONATHAN ZDZIARSKI, *IPHONE FORENSICS: RECOVERING EVIDENCE, PERSONAL DATA & CORPORATE ASSETS* (2008).

200. See Amber Hunt, *Latest Police Weapon: iWitness?*, USA TODAY, July 8, 2010, at 1A.

videos that show users how to access data on iPhones.<sup>201</sup> For some older versions of the phone, police only need to tinker with the device itself to bypass the password function altogether in a matter of moments. For newer versions of the iPhone (that have closed earlier loopholes), police can still hack into the phone using only a laptop, iTunes, and open-source forensic recovery software.<sup>202</sup> Even police departments with limited funds can scrounge up a laptop computer, and even inexperienced hackers can follow the simple directions posted on the Internet to bypass the password.

In the comfort of the police station, police could therefore gain access to the data on a password-protected cell phone in a matter of minutes. And while the iPhone only accounts for a sixteen percent share of the cell-phone market currently,<sup>203</sup> other popular cell phones also utilize four-digit pass codes that offer similarly limited protection.<sup>204</sup>

\* \* \*

At bottom, the fact that a phone is password protected does not legally or practically prevent it from being searched. Password protecting a cell phone places limited legal roadblocks in law enforcement's path—making it difficult to search the phone at the scene of arrest—but does not prevent quick searches at the scene or lengthier investigations at the station house. And while passwords appear to provide great protection that might deter law enforcement, with minimal effort police may be able to decipher or bypass the password to gain access to a phone's contents.

#### IV. THE IPHONE MEETS THE FIFTH AMENDMENT

As detailed in Part III, the search-incident-to-arrest doctrine provides police with the opportunity to guess or crack a cell phone's password in an effort to search it. What happens, however, if police are unable to break into the phone on their own? Can police ask or even demand that an arrestee enter the password himself or verbally provide it to the police? As explained

---

201. There are dozens of videos available on YouTube demonstrating how to bypass the iPhone's pass code. See, e.g., MrNerveGas, *Removing iPhone 3G[s] Passcode and Encryption*, YOUTUBE (July 24, 2009), <http://www.youtube.com/watch?v=5wS3AMbXRLs>; TatesMan, *How To Bypass iPhone's Passcode*, YOUTUBE (Aug. 28, 2008), <http://www.youtube.com/watch?v=OBUDSsp5U-4&feature=related>.

202. See ZDZIARSKI, *supra* note 199, at 19–42 (offering step-by-step instructions for using the iLiberty+ program to avoid the prohibition on installing software not signed by Apple and to thereafter install a forensic-recovery toolkit that will permit law enforcement to extract data from the phone).

203. See Antone Gonsalves, *Apple iPhone Gains Market Share, BlackBerry Slips*, INFORMATIONWEEK (May 10, 2010, 8:00 AM), [http://www.informationweek.com/news/mobility/smart\\_phones/showArticle.jhtml?articleID=224701204](http://www.informationweek.com/news/mobility/smart_phones/showArticle.jhtml?articleID=224701204).

204. See, e.g., VERIZON WIRELESS, VOYAGER USER GUIDE 116–18 (describing how to utilize “four-digit lock code”), available at [http://www.lg.com/us/mobile-phones/pdf/Voyager\\_UG\\_E\\_1.3.pdf](http://www.lg.com/us/mobile-phones/pdf/Voyager_UG_E_1.3.pdf).

below, while the law is complicated, in many cases police will be able to obtain the password without running afoul of the Fifth Amendment. If police request the password from an arrestee who is in custody, they have likely engaged in an interrogation that requires *Miranda* warnings. Yet, because the fruit-of-the-poisonous-tree doctrine does not apply to evidence discovered as a result of *Miranda* violations, police who fail to comply with *Miranda* suffer no consequences. As Part IV.B explains, if arrestees turn over their password in response to a police demand (as opposed to a voluntary request), the arrestee has only a weak argument that the police have violated the Fifth Amendment by compelling incriminating information. Moreover, many arrestees will never reach this point because they will consensually relinquish their password well in advance of a police demand.

A. *THE MIRANDA DOCTRINE MAY PROTECT AGAINST REQUESTS FOR PASSWORDS, BUT VIOLATIONS WILL NOT LEAD TO THE SUPPRESSION OF VALUABLE EVIDENCE*

The *Miranda* doctrine applies when an individual is in custody and subject to interrogation.<sup>205</sup> The interrogation element is easily satisfied. When a police officer asks an individual, “What is your password?” the inquiry constitutes an interrogation.<sup>206</sup> Moreover, even if the officer is clever enough to avoid phrasing the matter as a question (for instance, “Please tell me the password”), the Supreme Court has recognized that such functional equivalents of questioning amount to an interrogation if they are designed to elicit an incriminating response.<sup>207</sup> Accordingly, requesting that an arrestee voluntarily turn over the password to his phone (which may inculcate him by leading to evidence on the phone) amounts to interrogation.

The custody question is slightly more complicated. Although the Supreme Court has adopted different tests for determining whether a person is under arrest and whether they are in custody for *Miranda* purposes,<sup>208</sup> it seems clear that an individual is in custody if he has been

---

205. See *Miranda v. Arizona*, 384 U.S. 436, 444 (1966).

206. In *Rhode Island v. Innis*, the Supreme Court held that interrogation includes either express questioning or the functional equivalent of express questioning when the police should know the interaction is likely to elicit an incriminating response. 446 U.S. 291, 300–01 (1980). In the case’s aftermath, some courts have held that express questioning not likely to elicit an incriminating response did not amount to interrogation. See Meghan S. Skelton & James G. Connell, III, *The Routine Booking Question Exception to Miranda*, 34 U. BALT. L. REV. 55, 69–71 (2004). These holdings, however, appear to be a misreading of *Innis*, as the decision appears to indicate that all express questioning (whether or not it is likely to elicit an incriminating response) amounts to interrogation. See *id.* at 77.

207. *Innis*, 446 U.S. at 300–01.

208. See Thomas K. Clancy, *What Constitutes an “Arrest” Within the Meaning of the Fourth Amendment?*, 48 VILL. L. REV. 129, 173 (2003) (“[T]he concept of custody under *Miranda* and the Fourth Amendment’s measurement of what constitutes an arrest are not equivalent.”).

formally subjected to a full-scale custodial arrest.<sup>209</sup> Thus, if an officer requests the password to a phone during a search incident to arrest, the arrestee is also in custody for *Miranda* purposes.

One small wrinkle remains. The search-incident-to-arrest doctrine can apply even before an individual has been subjected to a custodial arrest.<sup>210</sup> In these circumstances, if police ask for a password as they begin searching a cell phone, but before they formally arrest an individual, the government might be able to argue that the individual was not yet in custody and therefore not entitled to *Miranda* warnings. In such a scenario, we would revert back to the general custodial standard that asks whether a reasonable person in the individual's shoes would perceive that his "freedom of action [was] curtailed to a 'degree associated with a formal arrest.'"<sup>211</sup>

It is, of course, possible to imagine a scenario in which an officer begins to search a phone before a reasonable person would realize that he is about to be arrested and transported to the police station. For example, an officer who stops a driver with reason to believe he is involved in a drug ring (and who sees the driver actively pushing buttons on his phone as the officer approaches the vehicle) might immediately grab the phone and request the password in the hope of preventing evidence from being destroyed before the arrestee is handcuffed and placed in the squad car. In this situation, the soon-to-be-arrested driver might not reasonably think he is in custody, and thus he would not be entitled to *Miranda* warnings even though a search incident to arrest is in fact underway.

While the above hypothetical is plausible, it seems quite unlikely. In drug cases, police almost always handcuff and secure arrestees immediately to protect their safety.<sup>212</sup> Thus, the number of instances in which an officer searches a phone incident to arrest and requests a password before formally placing the individual under arrest and in custody for *Miranda* purposes is likely to be extremely low. As such, when police request that an arrestee voluntarily turn over his cell-phone password, the arrestee is subject to

---

209. See George E. Dix, *Nonarrest Investigatory Detentions in Search and Seizure Law*, 1985 DUKE L.J. 849, 927 ("Miranda does apply to custodial—that is, 'arrest'—interrogations, even for minor offenses." (citing *Berkemer v. McCarty*, 468 U.S. 420, 441 (1984))).

210. *Rawlings v. Kentucky*, 448 U.S. 98, 111 (1980) ("Where the formal arrest followed quickly on the heels of the challenged search of petitioner's person, we do not believe it particularly important that the search preceded the arrest rather than vice versa."). For trenchant criticism of allowing searches to precede arrest, see Logan, *supra* note 153, at 405–14.

211. *Berkemer*, 468 U.S. at 440 (quoting *California v. Beheler*, 463 U.S. 1121, 1125 (1983) (per curiam)).

212. See Myron Moskowitz, *A Rule in Search of a Reason: An Empirical Reexamination of Chimel and Belton*, 2002 WIS. L. REV. 657, 665–66 (surveying California police agencies and documenting that "in general, police officers are taught to handcuff an arrestee (preferably behind his back) before searching the area around him").

custodial interrogation and any request for the password must be preceded by *Miranda* warnings.

Yet, as in many other cases, the *Miranda* requirement is a hollow protection, because the fruit-of-the-poisonous-tree doctrine<sup>213</sup> does not apply to *Miranda* violations.<sup>214</sup> While a confession that violates *Miranda* will be suppressed, evidence found thereafter is admissible. If police obtain an arrestee's password in violation of *Miranda*, an officer's statement conceding knowledge of the password will be inadmissible, but any valuable resulting evidence—for instance, incriminating text messages or child pornography found on the phone—will be admissible.

*B. POLICE DEMANDS FOR THE PASSWORD LIKELY DO NOT AMOUNT TO A VIOLATION OF THE FIFTH AMENDMENT'S SELF-INCRIMINATION CLAUSE*

A final problem worthy of attention is what happens if police demand (rather than request) that an arrestee provide his password and the arrestee complies out of a belief that he has no choice. In this scenario, have police compelled an arrestee to incriminate himself with a testimonial response in violation of the Fifth Amendment's protection against self-incrimination? Although the law is murky, the answer is probably "no."

To assert a Fifth Amendment self-incrimination challenge, an individual must demonstrate that (1) he has been compelled (2) to produce testimony (3) that is incriminating.<sup>215</sup> Taking the elements out of order, it is simple to satisfy the incrimination requirement. Although a password will almost never be incriminating by itself, the information it protects often will be. For over half a century, the Supreme Court has recognized that Fifth Amendment protection applies not only to responses that are themselves incriminating, but also to information that "would furnish a link in the chain of evidence needed to prosecute the claimant."<sup>216</sup> If providing the password leads to incriminating information, this element is satisfied.

It is much more challenging for a defendant to demonstrate the compulsion element. Ordinarily, when one thinks of a person being compelled to incriminate herself, it is not via police interrogation, but instead in the context of a grand-jury subpoena. Indeed, when police officers interrogate a suspect they lack the legal authority to compel the individual to say anything. As a result, it is not surprising that the only two

---

213. Under the fruit-of-the-poisonous-tree doctrine, evidence found as a result of a constitutional violation is (subject to a few exceptions) not admissible.

214. See *Oregon v. Elstad*, 470 U.S. 298 (1985).

215. See Susan W. Brenner, *Constitutional Rights and New Technologies in the United States*, in *CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES: A COMPARATIVE STUDY* 225, 231 (Ronald E. Leenes et al. eds., 2008).

216. *Hoffman v. United States*, 341 U.S. 479, 486 (1951).

cases in which defendants have been compelled to disclose their computer passwords have been in response to grand-jury subpoenas.<sup>217</sup>

The idea that police cannot compel incriminating testimony is further supported by the Supreme Court's recent decision in *Chavez v. Martinez*.<sup>218</sup> In *Chavez*, a plurality of the Court concluded that an individual who had been inappropriately interrogated could not raise a self-incrimination claim in a civil-rights lawsuit because the Government never filed criminal charges against him, and therefore he had not been forced to incriminate himself in a criminal case in violation of the Fifth Amendment.<sup>219</sup> Put differently, while police might have compelled information from Chavez, they did not do so for Fifth Amendment purposes because the protection against self-incrimination applies only to testimony used in criminal cases.

Further supporting the position that police cannot compel testimony is the fact that for the last century, cases alleging police misconduct during interrogations have almost universally been analyzed under the *Miranda* doctrine or under the Fifth and Fourteenth Amendments' Due Process Clauses, not the Self-Incrimination Clause.<sup>220</sup>

A contrary argument in favor of police authority to compel an incriminating response can be imagined by citing to the Supreme Court's 1897 decision in *Bram v. United States*, in which the Court recognized that the Fifth Amendment's Self-Incrimination Clause protects against police interrogation.<sup>221</sup> Add to that decision the fact that the Supreme Court adopted the *Miranda* doctrine largely because of the view that custodial interrogations are inherently compelling, and one can argue that police can compel an incriminating response.<sup>222</sup> The prospect of the police badgering an arrestee or demanding information to which they are not legally entitled seems like exactly the type of coercive situation the Fifth Amendment is intended to protect against. To suggest that police should be able to slide between the Fifth Amendment's Self-Incrimination Clause (because they are

---

217. *United States v. Kirschner*, Misc. No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

218. 538 U.S. 760 (2003).

219. *Id.* at 773 (plurality opinion).

220. If police cannot compel a password in violation of the Self-Incrimination Clause, an arrestee's only recourse would be to argue that any evidence is inadmissible because it was involuntarily coerced in violation of due process. As such, the arrestee would have to point to force, threat of force, or extreme psychological trickery to prevail. If all the arrestee can point to are persistent, but polite, police demands that the arrestee turn over the password, an involuntariness challenge will almost certainly fail.

221. 168 U.S. 532 (1897).

222. Indeed, in *Miranda*, the dissenting justices unsuccessfully maintained that the Fifth Amendment should not apply to police interrogations because police lacked the contempt power to compel answers. See Lawrence Herman, *The Unexplored Relationship Between the Privilege Against Compulsory Self-Incrimination and the Involuntary Confession Rule (Part II)*, 53 OHIO ST. L.J. 497, 530 (1992) (describing dissenting opinions of Justices Harlan and White).

not judicial officers) and the Due Process Clauses (because their demands for the password are not so forceful as to coerce the defendant) is contrary to the expressed purpose behind the *Miranda* doctrine.

While the police-compulsion argument has some allure, it is ultimately unpersuasive. In their book on police interrogation, Professors George Thomas and Richard Leo declined to discuss the Self-Incrimination Clause:

Our book is about the law of interrogation. What the Fifth Amendment contributes to the law of interrogation is *Miranda*. . . . [I]t is fair to say that, as far as the law of police interrogation in the United States is concerned, there is *Miranda* and there is the due process prohibition of involuntary confessions.<sup>223</sup>

In short, while it may seem incongruous that police could demand a password without violating the Fifth Amendment, the reality is that the Court's current jurisprudence makes *Miranda* the only Fifth Amendment remedy available to defendants. Accordingly, any self-incrimination claim arising out of a police demand for a cell-phone password should fail for lack of compulsion.

Assuming (contrary to the discussion above) that a defendant could prove police compulsion, he would still have to demonstrate that declaring the password was testimonial to assert a successful self-incrimination claim. When an individual provides a password, courts should consider this a testimonial act, although the sheer complexity of the analysis might lead judges to misconstrue the law.

Evidence is testimonial (and thus protected by the Fifth Amendment) if it causes an individual "to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government."<sup>224</sup> The Court has recognized that most verbal statements "convey information or assert facts" and therefore "[t]he vast majority of verbal statements thus will be testimonial."<sup>225</sup> By contrast, when an individual is not asked to reveal the contents of his mind, as when he displays physical characteristics like the sound of his voice or his physical appearance, the evidence is nontestimonial.<sup>226</sup> Asking a suspected drunk driver if he has been drinking calls for a testimonial response, whereas taking a sample of his blood only represents a physical trait that is nontestimonial.<sup>227</sup>

---

223. See E-mail from George C. Thomas III, Bd. of Governors Professor of Law & Judge Alexander P. Waugh, Sr. Distinguished Scholar, Rutgers Sch. of Law–Newark, to Adam Gershowitz, Assoc. Professor of Law, Univ. of Hous. Law Ctr. (Sept. 6, 2010, 2:37 PM) (on file with author) (quoting GEORGE C. THOMAS III & RICHARD A. LEO, *THE HISTORY AND FUTURE OF INTERROGATIONS* ch. 3 (forthcoming 2011)).

224. *Doe v. United States*, 487 U.S. 201, 213 (1988).

225. *Id.*

226. See *Pennsylvania v. Muniz*, 496 U.S. 582, 594–95 (1990).

227. See *Schmerber v. California*, 384 U.S. 757, 761 (1966).

In light of frequently quoted dicta from a 1988 Supreme Court decision, it seems clear that asking an arrestee to disclose his password is testimonial. In *Doe*, the Court noted that forcing an arrestee to turn over the key to a strongbox containing incriminating documents would not be testimonial, whereas compelling him to turn over the combination to a wall safe would be.<sup>228</sup>

The Court's logic in *Doe* is not detailed or particularly persuasive, although it reaches the correct conclusion that reciting a password is testimonial. First, it is important to recognize that, contrary to the Court's suggestion, turning over the key to a strongbox could also be testimonial. Courts have repeatedly held that producing tangible evidence, such as a murder weapon or a victim's body, can be testimonial even in the absence of any verbal language.<sup>229</sup> This is because producing such tangible evidence demonstrates the existence, control, and location of those items, which amounts to testimony.<sup>230</sup> In the cell-phone context, this is significant because clever police officers could attempt to avoid a Fifth Amendment problem by demanding that an arrestee either provide a written copy of his password or simply enter the password himself without the officer seeing it.<sup>231</sup> Indeed, in one of only two cases addressing the compulsion of computer passwords, prosecutors offered to have the individual enter his password without any onlookers, so that he would not have to make a testimonial statement in violation of the Fifth Amendment.<sup>232</sup> The magistrate assigned to the case refused to accept this option, explaining that even entering the password privately would be testimonial because it would demonstrate knowledge of the password and access to the underlying computer files.<sup>233</sup>

Despite the Supreme Court's ill-advised comment that the key to a strongbox would not be testimonial, the Court was correct in concluding the combination to a safe is testimonial. Prosecutors might argue that a password is not testimonial because it does not convey an arrestee's thoughts or beliefs, or cause him to reveal knowledge relating him to a criminal offense.<sup>234</sup> This position is incorrect because providing the password would reveal the contents of an arrestee's mind by recalling the password. Indeed, even if an arrestee only had to produce a preexisting copy of the password (e.g., one previously written on a post-it note or saved on a zip drive), the act of producing that item would demonstrate the existence and control of the

---

228. *Doe*, 487 U.S. at 210 n.9.

229. *See, e.g.*, *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1244-45 (Mass. 1980).

230. *Fisher v. United States*, 425 U.S. 391, 410 (1976).

231. I am grateful to Professor Susan Brenner for making this point to me.

232. *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473, at \*2 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

233. *See id.* at \*4.

234. *See Doe v. United States*, 487 U.S. 201, 213 (1988).

password, and by implication, an arrestee's knowledge of the contents of the cell phone.<sup>235</sup> Put simply, providing the password to a cell phone—whether from an individual's mind, a post-it note in his pocket, or by inputting it with his own hand—should be considered testimonial.

In sum, a police demand for an arrestee's password can certainly be testimonial and incriminating, but the self-incrimination claim should probably fail because the defendant is unable to demonstrate compulsion. Accordingly, an arrestee who turned over his password in response to police demands has, at best, a very weak argument that his Fifth Amendment protection against self-incrimination has been violated.<sup>236</sup> Moreover, even if a court reaches a contrary conclusion on the compulsion question and thus finds a self-incrimination violation, there are at least three additional reasons to believe Fifth Amendment protection of the password is of minimal value.

First, most arrestees will never be in a position to assert a self-incrimination claim because they will have revealed the password voluntarily. If police simply ask, rather than demand, that an arrestee enter the password to his phone and he consents, there is no compulsion and hence no Fifth Amendment violation. As explained above, while police should be obligated to read an arrestee his *Miranda* warnings before requesting his password, in reality, the warnings provide virtually no protection because individuals typically waive them.<sup>237</sup> Moreover, even if police failed to read the warnings, the fruit-of-the-poisonous-tree doctrine does not require suppression of evidence subsequently found on the phone. Only the statement identifying the password (a confession that, by itself, is nearly valueless in a criminal prosecution) would be suppressed.<sup>238</sup>

Second, if an officer is unable to convince an arrestee to turn over the password consensually and badgers the arrestee to turn over the password enough that there is arguably compulsion under the Fifth Amendment, the State may nevertheless argue that the contents of the phone are not testimonial because they were a "foregone conclusion." The Supreme Court has recognized that when police ask an individual to produce evidence that is already known to the Government (and thus a "foregone conclusion"),

---

235. See Susan Brenner, *Miranda, the 5th Amendment, and Cell Phones*, CYB3RCRIM3 (July 26, 2010, 1:01 PM), <http://cyb3rcrim3.blogspot.com/2010/07/miranda-5th-amendment-and-cell-phones.html>.

236. See 1 JOSHUA DRESSLER & ALAN C. MICHAELS, *UNDERSTANDING CRIMINAL PROCEDURE* § 22.03[C][2][b] (4th ed. 2006).

237. See Richard A. Leo, *Inside the Interrogation Room*, 86 J. CRIM. L. & CRIMINOLOGY 266, 276 (1996) (finding that seventy-eight percent of suspects in a study of a major urban police department waived their *Miranda* rights).

238. See *supra* notes 213–14 and accompanying text.

the act of production is not testimonial.<sup>239</sup> For example, the Government might argue that police observed an arrestee texting on his phone immediately before a drug bust and that it was apparent that the text messages were being used to facilitate drug deals. The prosecutor might therefore argue that any incriminating text messages were a foregone conclusion and that the password did not provide any unanticipated information, and thus the compelled evidence is not testimonial.

The foregone-conclusion argument should fail in the vast majority of cases, because without knowing the specific contents of the phone, police are not in a position to say before the search what evidence will be found once the arrestee enters his password. Under the Supreme Court's decision in *United States v. Hubbell*, a simple Government assertion that incriminating information exists is not sufficient to demonstrate a foregone conclusion.<sup>240</sup> In *Hubbell*, the Government asserted that a subpoena to a businessman to produce thousands of pages of business and tax documents was not testimonial because the existence and location of the documents was a foregone conclusion given that businessmen always possess general business and tax records.<sup>241</sup> The Supreme Court rejected this argument on the grounds that its vague assertion failed to demonstrate the existence and whereabouts of the actual documents ultimately produced by Hubbell.<sup>242</sup>

In light of the specificity required by *Hubbell*, prosecutors will likely be unsuccessful in making vague assertions that the contents of text messages on a cell phone are a foregone conclusion. With the exception of long-term investigations in which police know of specific information on the phone and simply lack the time to get a warrant, courts should reject the foregone-conclusion doctrine. Nevertheless, because this area of law is complicated and murky, it would not be surprising to see courts incorrectly adopt the foregone-conclusion approach in borderline cases where police had some inclination that cell phones contained illegal, but unspecified, information.

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."<sup>243</sup> In *Chavez*, an arrestee was shot by police and subsequently interrogated while receiving medical treatment, even though he had not

---

239. *Fisher v. United States*, 425 U.S. 391, 411 (1976) ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

240. 530 U.S. 27, 44-45 (2000).

241. *Id.* at 44.

242. *See id.* at 44-46.

243. 538 U.S. 760, 764-65 (2003) (plurality opinion).

received his *Miranda* warnings.<sup>244</sup> Chavez made incriminating statements, but he was never charged with a crime.<sup>245</sup> In a subsequent civil-rights lawsuit against the police department, Chavez alleged a violation of his Fifth Amendment rights.<sup>246</sup> The Supreme Court rejected Chavez's claim, with Justice Thomas explaining for a plurality that it "does not violate the text of the Self-Incrimination Clause absent use of the compelled statements in a criminal case against the witness."<sup>247</sup> Because legal proceedings were never initiated against Chavez, he was not forced to incriminate himself in a "criminal case" and thus suffered no Fifth Amendment violation.<sup>248</sup> Under *Chavez*, if police compel a password and search a phone but find no evidence, arrestees are seemingly without a remedy for the forced compulsion of the password. Individuals remain free to bring a civil-rights lawsuit based on a Fourth Amendment claim, but because most courts have held that searching a cell phone incident to arrest is lawful, any argument premised on the Fourth Amendment will currently fail.<sup>249</sup>

In sum, the Fifth Amendment issues arising out of a police demand for an arrestee's password raise complex and unresolved questions. An arrestee can make only a weak claim that complying with a police demand for a password violates the Self-Incrimination Clause because he will be unable to demonstrate the necessary element of compulsion. Even if his claim is viable as a purely legal matter, in practice it will rarely prevail. Most arrestees will have turned over their passwords voluntarily, and in other cases courts may incorrectly side with the government based on the foregone-conclusion doctrine. At bottom, arrestees likely have little or no self-incrimination protection against police demands for cell-phone passwords.

## V. CONCLUSION

Password protecting your cell phone is undoubtedly a good idea. If the phone is lost, the password will help to protect the data. And if you are arrested, the password will make it more difficult for police officers to search the phone incident to arrest. But password protecting the phone will not necessarily prevent the police from bypassing the password and conducting a warrantless search of the phone. As a legal matter, password protecting the phone provides virtually no additional protection against police searches of cell phones incident to arrest. Longstanding caselaw permits police to attempt to open locked containers when searching incident to arrest, and by analogy, police are able to attempt to access the contents of a password-

---

244. *Id.*

245. *Id.* at 764.

246. *Id.* at 764-65.

247. *Id.* at 769.

248. *Id.* at 766.

249. *See supra* Part II.B.1.

protected phone. Even if police cannot decipher the password on their own, they stand a strong chance of acquiring the password from simple police interrogation. Requesting a password requires police to give an arrestee *Miranda* warnings, but many individuals waive their *Miranda* rights and, in any event, violations of *Miranda* do not lead to suppression of evidence subsequently found. Arrestees likewise have little chance of successfully asserting a Fifth Amendment self-incrimination claim because police are not judicial officers and lack the authority to “compel” incriminating information in violation of the Self-Incrimination Clause. Moreover, because cell phones are often found on the person of an arrestee, police can bring them to the station, where computer-savvy officers can spend hours attempting to hack into the phone without first procuring a warrant.

Police currently have wide latitude to search the contents of cell phones—including text messages, voicemails, photos, Internet browsing history, and reams of other data—when searching an arrestee incident to arrest. Given that password protecting the phone does little to curb this police power, the Supreme Court and legislatures should undertake efforts to scale back the ability of law enforcement to search digital devices incident to arrest.<sup>250</sup>

---

250. See Gershowitz, *supra* note 1, at 45–57 (suggesting potential legislative and judicial solutions).