

William & Mary Law School

## William & Mary Law School Scholarship Repository

---

Popular Media

Faculty and Deans

---

11-2011

### Can Police Search Your Cell Phone, and Even Break Your Password, During an Arrest?

Adam M. Gershowitz

*William & Mary Law School*, [amgershowitz@wm.edu](mailto:amgershowitz@wm.edu)

Follow this and additional works at: [https://scholarship.law.wm.edu/popular\\_media](https://scholarship.law.wm.edu/popular_media)

---

#### Repository Citation

Gershowitz, Adam M., "Can Police Search Your Cell Phone, and Even Break Your Password, During an Arrest?" (2011). *Popular Media*. 292.

[https://scholarship.law.wm.edu/popular\\_media/292](https://scholarship.law.wm.edu/popular_media/292)

Copyright c 2011 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

[https://scholarship.law.wm.edu/popular\\_media](https://scholarship.law.wm.edu/popular_media)



Composite: MicroWorks; Giorgio Magini; Hanibaram | istockphoto.com

## Can Police Search Your Cell Phone, and Even Break Your Password, During an Arrest?

Over the last decade, cell phone use has exploded. Many Americans now carry incredible amounts of information in their phones, including pictures, documents, music, text messages, and emails. 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.

This is a condensed version of a previously published article. Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone From a Search Incident to Arrest?*, 96 IOWA L. REV. 1125 (2011) (reprinted with permission).

In recent years, prosecutors have sought to admit evidence from cell phone searches based on the search incident to arrest doctrine. That doctrine — which has been used by police on the street for decades — allows police to conduct a complete search of the items on an arrestee following any custodial arrest. Searching cell phones following an arrest obviously gives law enforcement access to far more information than a traditional search of a wallet or jacket pocket. Yet many courts have agreed with prosecutors and upheld cell phone searches incident to arrest, even if there was no reason for law enforcement to believe the phone contained evidence related to the arrest.

This article discusses the stunningly broad scope of the search incident to arrest doctrine as applied to cell

phones. After explaining why current Supreme Court precedent seemingly authorizes such broad searches, the article goes a step further and explores a question that courts have not yet been forced to confront: Can police search cell phones that have been password protected? Password-protected phones raise tough issues, including whether police can try to break a password themselves without an owner's consent, and whether they can demand that an arrestee turn over the password without violating *Miranda* or the Fifth Amendment protection against self-incrimination. Although the answers to these questions are tricky, the bottom line is that police authority under the search incident to arrest doctrine is so vast that even password protecting the phone leaves defendants with minimal legal protection. In the end, if the Supreme Court maintains its current search incident to arrest doctrine, little will stand in the way of police extracting enormous information from defendants' cell phones, even without a warrant or probable cause.

### The Supreme Court's Search Incident to Arrest Doctrine

The starting point for the broad search incident to arrest doctrine is the Supreme Court's 1969 decision in *Chimel v. California*.<sup>1</sup> In *Chimel*, the Court suppressed evi-

BY ADAM M. GERSHOWITZ



dence found when police searched Ted Chimel's entire home, including his attic and garage, following an arrest for burglary. 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 officer and to prevent an arrestee from concealing or destroying evidence. The Court limited the scope of the search to the arrestee's person and the area within his immediate control from which he might gain possession of a weapon or destroy evidence. Thus, while police could not rummage through Chimel's entire house following arrest, they were free to search anywhere on his person or 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>2</sup> Police arrested Willie Robinson for the crime of operating a motor vehicle with a revoked license. 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. The officer reached into the pocket and pulled out a crumpled cigarette package. Still unsure what was in the package, the officer opened it and discovered capsules of heroin. 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. The Court announced a bright-line rule 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 if the officers have no suspicion that the contents of the container are illegal.

In its next series of important search incident to arrest decisions, the Supreme Court turned its attention to automobiles. In the first case — *New York v. Belton*<sup>3</sup> — 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. In *Belton*, the officer stopped a car for speeding and, upon smelling marijuana, arrested the occupants. 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. The officer unzipped the jacket pockets and found cocaine. In upholding the search of the jacket, the Court explained the value of “a straightforward rule, easily applied and predictably

enforced.”<sup>4</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 containers inside the vehicle regardless of whether they could contain a weapon or evidence of a crime.

After years of expanding the scope of the search incident to arrest doctrine, the Supreme Court scaled back police authority to search vehicles incident to arrest in 2009. In *Arizona v. Gant*,<sup>5</sup> police arrested the defendant for driving with a suspended license, handcuffed him, and placed him in the back of a police car. Thereafter, police searched Rodney Gant's vehicle and found a jacket in the backseat that contained cocaine. The *Gant* Court narrowed the *Belton* rule and held that police can only search a vehicle incident to arrest if “the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search” or if “it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.”<sup>6</sup> While the *Gant* decision is clearly an effort to narrow the search incident to arrest doctrine, at present the decision is only applicable to searches of vehicles and it is debatable how much change it will foster.

## Searching Cell Phones Incident to Arrest

As wireless technology has become ubiquitous, courts have been called upon to apply the search incident to arrest doctrine to digital devices. The first such cases began to appear 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*,<sup>7</sup> police activated a pager and retrieved telephone numbers that linked Sam Chan to a drug ring. The federal court upheld the search of Chan's pager because it was nothing more than an electronic container and Supreme Court precedent authorized the search of containers incident to arrest. The court further explained that it was irrelevant that the arrestee could not retrieve a weapon from the pager nor plausibly destroy any evidence from the pager. 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. Following *Chan*, half a dozen other courts upheld similar searches of pagers.<sup>8</sup>

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

Although it is impossible to know how many cell phone searches have been conducted incident to arrest over the last few years, the number is likely in the thousands.<sup>9</sup> In many instances, police likely found nothing incriminating and in other cases defendants likely pleaded guilty without challenging the constitutionality of the searches. Nevertheless, more than 50 defendants have challenged the warrantless search of early generation cell phones over the last few years. In a handful of cases, courts have addressed whether these warrantless searches were permissible under the automobile exception,<sup>10</sup> the inventory exception,<sup>11</sup> the exigency exception,<sup>12</sup> or based on consent.<sup>13</sup> The bulk of warrantless cell phone searches, however, have been decided under the search incident to arrest doctrine, and courts have upheld the searches in the vast majority of cases.<sup>14</sup>

The most prominent case upholding the search incident to arrest of a cell phone is the Fifth Circuit's decision in *United States v. Finley*.<sup>15</sup> After arresting Jacob Finley as part of a staged drug sale, police searched the cell phone in his pocket incident to arrest. Officers found incriminating text messages related to drug trafficking, and Finley was subsequently convicted.

On appeal, Finley contended that the search of his cell phone was unlawful because the Fourth Amendment permitted only the seizure, not the warrantless search, of his phone. Just as in the pager context, the Fifth Circuit refused to draw a distinction between wireless technology and searches of more traditional containers. The court explained that “police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial.”<sup>16</sup> In short, the Fifth Circuit did not recognize any conceptual difference between search-



ing physical containers for drugs and searching electronic equipment for digital information.

Although the *Finley* decision has been cited repeatedly as the leading decision, a small number of courts have refused to follow its reasoning.<sup>17</sup> These courts have employed a variety of rationales in rejecting warrantless searches of cell phones.

The Ohio Supreme Court, in a recent and closely divided 4-3 opinion, is the most prominent court to reject the search incident to arrest of cell phones.<sup>18</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. 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 inside. The four-justice majority maintained that to be a container under the Supreme Court's decision in *Belton*, the item must be capable of holding a "physical object within it."<sup>19</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>20</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>21</sup>

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*, the defendant was arrested on drug charges and brought to the police station.<sup>22</sup> At the station, approximately 90 minutes following the arrest, the police searched his cell phone and located incriminating information. 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>23</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>24</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 or a cigarette package in a pocket, and searches of possessions within an arrestee's immediate control, such as a footlocker. 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, not later at the police station. The *Park* court then determined that because of the sheer volume of private information held on cell phones, they should be considered possessions within the arrestee's immediate control. And because the search incident to arrest of *Park's* cell phone occurred at the station, it was impermissible.

At least two 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>25</sup> In *Gant*, the Supreme Court restricted searches incident to arrest of automobiles to situations in which "the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search" or "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."<sup>26</sup> The Court's decision in *Gant* was clearly limited to searches of automobiles incident to arrest, but these two 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 and occurred too long after 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>27</sup> Eventually, an officer answered the phone and heard the caller attempt to buy drugs. Relying in part on the fact that the officer answered the phone 20 minutes after arrest, a Massachusetts court suppressed evidence of the phone call because it occurred too long after arrest to be contemporaneous. 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 after the suspect was initially arrested.<sup>28</sup> The court concluded that such a time peri-

od was not contemporaneous with arrest and suppressed the evidence.<sup>29</sup> Importantly, these contemporaneousness cases limit, but do not outrightly forbid, the search incident to arrest of cell phones.

## Can a Password Save Your Cell Phone From the Search Incident to Arrest Doctrine?

As members of the public increasingly become aware that police are conducting warrantless cell phone searches following arrests, they will likely begin to password protect their phones. To date, courts have not been called upon to address police authority to bypass passwords during searches incident to arrest, but that issue will surely arise in the near future.

## 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 without the owner's permission in order to access the data on the phone. The answer to this question depends on whether police have authority to break into a locked container.

Although the search incident to arrest doctrine has existed for over 70 years, the Supreme Court has never clearly stated whether police are permitted to unlock 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 could search "any" containers, whether "open or closed."<sup>30</sup> And the dissenting justices in *Belton* clearly expressed their belief that the decision extended to locked containers.<sup>31</sup>

In the years since *Belton*, there has been a fair amount of consensus among lower courts permitting police to enter locked containers as long as the officers do not irreparably damage them. For example, over the last three decades, courts have almost unanimously<sup>32</sup> held that police may open locked glove compartments during searches incident to arrest.<sup>33</sup>

Some courts have gone beyond glove compartments to permit searches incident to arrest of even more secure containers such as locked safes,<sup>34</sup> locked footlockers,<sup>35</sup> locked briefcases,<sup>36</sup> boxes sealed with tape,<sup>37</sup> and locked overnight bags.<sup>38</sup>

Based on these decisions, it would seem clear that police can attempt to crack a cell phone password during a search



incident to arrest. Just as police are permitted to try all of the keys on the defendant's keychain until locating the one that unlocks the glove compartment, police should be able to try multiple different combinations in an effort to discover the password to the phone.

## How Long Can Police Spend Trying to Crack a Password?

Assuming that police can search a password-protected phone, a harder question is how long they can take in trying to break the password. Unfortunately, the Supreme Court has never established any clear guideposts for what constitutes a contemporaneous search. And, in fact, the Court has created a confusing rule whereby the length of time depends on whether the police are searching an item on the person of an arrestee, as opposed to property near the arrestee.

## Searching Items Associated With the Person and Items That Are Merely Nearby Possessions

In determining how long police can spend trying to crack a password, the best

place to begin is the question of whether cell phones are items immediately associated with the arrestee or merely possessions near the arrestee. This distinction requires us to parse two Supreme Court cases from the 1970s.

In the somewhat obscure Supreme Court case of *United States v. Edwards*, police arrested Eugene Edwards at 11 p.m. for attempting to break into a government building.<sup>39</sup> Edwards was promptly brought to jail, processed, and placed in a cell. 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. The following morning, 10 hours after his arrest, police took Edwards' clothing from him to search for paint chips. 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. The Court rejected Edwards' argument and gave police wide authority to conduct the search incident to arrest well after the arrest was conducted.

Three years later, in the far more famous Supreme Court case of *United States v. Chadwick*, officers arrested Joseph Chadwick as he was trying to load a double-locked footlocker into his vehicle.<sup>40</sup>

One set of agents brought Chadwick to a federal building and another group of agents followed behind with the footlocker. Approximately 90 minutes after the arrest, federal agents opened the footlocker and discovered a large quantity of marijuana. 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>41</sup> The Court further explained that "[o]nce 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>42</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, howev-



## THE SWIFT HAND OF JUSTICE HOLDS A SMARTPHONE.

Being able to consult with your colleagues on the go gives you a resource beyond any law book. Real-life experience and knowledge of the law is invaluable in the pursuit of justice. And Verizon gives you access to that support system from your main office or your mobile one.

**Members of the National Association of Criminal Defense Lawyers** who belong to NPP may receive **up to 22% off** monthly access on Verizon Wireless. One- or two-year line term on eligible Calling Plans <sup>34</sup> or higher, and five wireless lines required.\*

Contact NPP-Legal Customer Service for more information.

1.800.810.3909

customerservice@mynpp.com

www.mynpp.com



\* Activation fee/line: up to \$35. Subject to Corporate Agreement, Calling Plan and credit approval. Coverage, varying by service, not available everywhere; see [vzw.com](http://vzw.com). ©2011 Verizon Wireless.



er, 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 decisions in *Edwards* and *Chadwick*, the Supreme Court has offered no additional guidance.

Decisions by lower courts, however, have concluded that many items are associated with the person of an arrestee. In addition to clothing, courts have concluded that wallets,<sup>43</sup> purses,<sup>44</sup> duffelbags,<sup>45</sup> and backpacks<sup>46</sup> fall under *Edwards* because they more closely resemble items on the person rather than nearby possessions like the footlocker in *Chadwick*.

## Cell Phones Will Often Be Associated With The Person, Allowing a Lengthy Time to Search

In order to determine how long police can spend trying to crack a cell phone password, courts must first determine whether the phone falls under *Edwards* or *Chadwick*. Most courts deciding searches incident to arrest of cell phones have not addressed this question, and the ones 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 how long they take to search the phones incident to arrest.<sup>47</sup> Once again, the key case supporting this approach is the Fifth Circuit's decision in *United States v. Finley*.<sup>48</sup> The Fifth Circuit specifically held that Finley's phone should not fall into the *Chadwick* category of nearby possessions because the cell phone "was on his person at the time of his arrest."<sup>49</sup>

By contrast, a federal court in California concluded that cell phones fell into the *Chadwick* box and rejected a search conducted 90 minutes after arrest at the police station. In *United States v. Park*, police arrested the defendant on marijuana charges and transported him to the police station.<sup>50</sup> As Edward Park was being booked, police removed a cell phone from him and placed it into an envelope for safekeeping. Because the investigating officer believed the phone might have evidence of marijuana trafficking, he instructed other officers to search it. The *Park* court concluded that cell phones "should be considered 'possessions within an arrestee's immediate control' and not part of 'the person.'"<sup>51</sup> The court reached this conclusion because:

[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>52</sup>

In the battle between the *Finley* reasoning (that cell phones are associated with the person of the arrestee) and the *Park* view (that phones are merely nearby possessions), the *Park* court appears to have the weaker side of the argument. First, 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 that can be searched at the station house under *Edwards*. When a cell phone is found in an arrestee's pocket, precedent therefore strongly suggests it should be searchable at the station house under *Edwards*.

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. Yet, the court offered no explanation why the quantity of information held in a phone had anything to do with whether it was associated with his person or merely a nearby possession. If a large quantify of information precluded an item from being associated with the person of an arrestee, then arguably a wallet should be categorized similarly because it contains information about 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 iPhone securely strapped to their arms. It is difficult to comprehend how a cell phone that is literally attached to an arrestee's arm

could not be associated with the person of an arrestee. Yet, under the *Park* court's reasoning, cell phones could never be associated with the person of the arrestee because they contain too much data.

In some instances, such as cases where the phone is found 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. Yet, 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 absolute answer to the question of whether a cell phone should be considered an item associated with the person of an arrestee (that can be searched hours after arrest under *Edwards*) or merely a nearby possession (that must be searched shortly after arrest under *Chadwick*). The best answer is simply that the categorization depends on the specific facts of the case. In some instances police should be permitted to search the cell phone hours after arrest at the police station, whereas in other cases such elongated searches should be forbidden.

## How Long Can Police Spend Searching Cell Phones Before the Search Ceases To Be Contemporaneous?

Even if cell phones are possessions near an arrestee that can be searched for only a short period of time under *Chadwick*, a determination still must be made regarding how long officers can search at the scene of the arrest. Are officers limited to five minutes after arrest, or can police officers take much longer? Unfortunately, there is no clear answer to this question.

Although the Supreme Court has trumpeted the need for bright-line rules in the search incident to arrest context, the Court has refused to adopt a bright-line rule dictating how long police can take to conduct such searches.<sup>53</sup> Not surprisingly, lower court decisions often appear to be completely inconsistent with one another.<sup>54</sup>

While courts have refused to draw bright-line time limits on searches incident to arrest, the contours of the case law do suggest that there is an outer time limit in run-of-the-mill cases. It is easy to locate hundreds of (non-cell phone) cases in which courts permitted searches incident to arrest five, 10, 20, and even 60 minutes, after arrest.<sup>55</sup> But very few cases involve searches more than an hour after



arrest.<sup>56</sup> The absence of such cases suggests that there truly is an implicit outer limit on the time to conduct searches incident to arrest.

## 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 the 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 for hours after the arrest. If police discover a cell phone within the grabbing space of an arrestee, such as in a briefcase or on the passenger seat of an automobile, they may search it but typically must do so at the scene and likely within minutes or at most an hour of 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 in the pocket of an arrestee. As explained below, they will have trouble doing the former, but could accomplish the latter.

If a cell phone must be searched on the scene and police have only a few minutes to do so, the password will likely prevent the police from accessing the phone's contents. In most cases, police will not be able to decipher the password during the commotion of an arrest. That said, it is possible that police could occasionally guess the password. One in five Americans uses an overly simplistic password such as "123456"<sup>57</sup> and an officer might simply get lucky by trying the most common passwords. Additionally, officers have access to an arrestee's driver's license that contains his birth date and home address, both of which are commonly used as passwords. Thus, while the chances of an officer cracking the password in a short time on the scene are limited, it is possible.

In the cases where police bring the cell phone to the station house because it is part of the arrestee's person, 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 10 times.<sup>58</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 blunt force computer program that sequentially inputs every numerical combination. 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 the technology becomes more available.

Moreover, even if police never set up the program to crack a password, 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" that explains how to remove data from the phone.<sup>59</sup> The same hacker proudly advertises that he teaches courses to law enforcement agencies, including lessons on bypassing passcodes.<sup>60</sup>

Even if police agencies lack the money or time to enroll any of their officers in computer forensics classes, they can turn to the numerous Internet videos that show users how to access the data on the iPhone.<sup>61</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 phone that have closed earlier loopholes, police can still hack into the phone and would only need a laptop, iTunes, and open source forensic recovery software.<sup>62</sup> 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.

## The iPhone Meets the Fifth Amendment

What happens if police are unable to break the password on their own? Can police ask or even demand that an arrestee enter the password himself or verbally provide the password? Defense counsel will be forced to confront two legal issues: (1) whether the *Miranda* doctrine offers any legal protection, and (2) whether police compulsion of the password violates the Fifth Amendment protection against self-incrimination.

As is often the case, the *Miranda* doctrine is not particularly helpful to the

defendant. While an arrestee is almost certainly in custody and a request for the password almost always will amount to interrogation,<sup>63</sup> invoking *Miranda* serves little purpose because the fruit of the poisonous tree doctrine does not apply to *Miranda* violations.<sup>64</sup> While a confession that violates *Miranda* will be suppressed, evidence found thereafter will be admissible. Thus, if police obtain an arrestee's password in violation of *Miranda*, the statement conceding knowledge of the password will be barred, but the valuable resulting evidence — the incriminating text messages or child pornography found on the phone — will be admissible.

An arrestee will also have a problem seeking relief under the Fifth Amendment's self-incrimination clause. While police badgering an arrestee into disclosing his password would seem like a quintessential Fifth Amendment violation, the Supreme Court would likely reject such a claim because, hard as it is to imagine, police lack the authority to compel an incriminating response for Fifth Amendment purposes. In a 2003 plurality decision, the Supreme Court concluded that an individual who had been improperly interrogated could not raise a self-incrimination claim in a civil rights lawsuit because no criminal charges had ever been filed against him and therefore he had not been compelled to incriminate himself in a criminal case in violation of the Fifth Amendment.<sup>65</sup> Put differently, while police might have forced the individual to provide information, they did not compel him for Fifth Amendment purposes because the protection against self-incrimination applies only to testimony in criminal cases. Perhaps for this reason, the only two cases in which defendants have been compelled to disclose their computer passwords have been in response to grand jury subpoenas, not police interrogation.

Accordingly, an arrestee who turned over his password in response to police demands would not have a strong argument that his Fifth Amendment protection against self-incrimination had been violated.

## Conclusion

Password protecting a cell phone is undoubtedly a good idea. If the phone is lost, the password will help to protect the data. And if an individual is 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 searching a cell phone incident to arrest. Longstanding case law permits police to attempt to open locked containers when searching incident to arrest. 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. Moreover, even if police cannot decipher the password on their own, they stand a strong chance of acquiring the password from simple police interrogation.

In sum, police in many jurisdictions have wide authority 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 police power, the Supreme Court and legislatures should undertake efforts to scale back law enforcement's authority to search digital devices incident to arrest.

## Notes

1. 395 U.S. 752 (1969).
2. 414 U.S. 218 (1973).
3. 453 U.S. 454 (1981).
4. *Id.* at 459.
5. 129 S. Ct. 1710 (2009).
6. *Id.* at 1719.
7. 830 F. Supp. 531 (N.D. Cal. 1993).
8. See *United States v. Hunter*, 1998 WL 887289 (4th Cir. Oct. 29, 1998); *United States v. Ortiz*, 84 F.3d 977 (7th Cir. 1996); *United States v. Stroud*, 1994 WL 711908 (9th Cir. Dec. 21, 1994); *United States v. Diaz-Liazaraza*, 981 F.2d 1216 (11th Cir. 1993); *United States v. Reyes*, 922 F. Supp. 818 (S.D.N.Y. 1996); *United States v. Lynch*, 908 F. Supp. 284 (D. V.I. 1995).
9. See *United States v. Wall*, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008), at \*12 (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").
10. See *United States v. Monson-Perez*, 2010 WL 889833 (E.D. Mo. Mar. 8, 2010); *United States v. Rocha*, 2008 WL 4498950 (D. Kan. Oct. 2, 2008); *United States v. James*, 2008 WL 1925032 (E.D. Mo. Apr. 29, 2008); *United States v. Fierros-Alvarez*, 2008 WL 1826188 (D. Kan. Apr. 23, 2008); *People v. Chho*, 2010 WL 1952659 (Cal. App. 6 Dist. May 17, 2010); *State v. Boyd*, 992 A.2d 1071 (Conn. 2010); *State v. Novicky*, 2008 WL 1747805 (Minn. App. Apr.

15, 2008).

11. See *United States v. Chappell*, 2010 WL 1131474 (D. Minn. Jan. 12, 2010); *United States v. Wall*, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008).

12. See *United States v. Salgado*, 2010 WL 3062440 (S.D. Ga. June 12, 2010).

13. See *United States v. Dobbs*, 2011 U.S. Dist. LEXIS 31171 (N.D. Ga. Feb. 3, 2011); *Lemons v. State*, 298 S.W.3d 658 (Tex. Ct. App. 2009); *United States v. James*, 2008 WL 1925032 (E.D. Mo. Apr. 29, 2008); *United States v. Galante*, 1995 WL 507249 (S.D.N.Y. Aug. 25, 1995).

14. For cases approving the search of cell phones incident to arrest, see *United States v. Curtis*, 2011 U.S. App. LEXIS 5002 (5th Cir. Mar. 11, 2011); *United States v. Pineda-Areola*, 2010 WL 1490369 (7th Cir. Apr. 6, 2010); *United States v. Fuentes*, 2010 WL 724186 (11th Cir. Mar. 3, 2010); *United States v. Murphy*, 552 F.3d 405 (4th Cir. 2009); *Silvan W. v. Briggs*, 2009 WL 159429 (10th Cir. Jan. 23, 2009); *United States v. Young*, 2008 WL 2076380 (4th Cir. May 15, 2008); *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007); *United States v. Hill*, 2011 WL 90130 (N.D. Cal. Jan. 10, 2011); *United States v. Grooms*, 2011 WL 381036 (E.D. Tenn. Jan. 3, 2011); *United States v. Rodriguez-Gomez*, 2010 WL 5524891 (N.D. Ga. Nov. 15, 2010); *United States v. Faller*, 681 F. Supp. 2d 1028 (E.D. Mo. 2010); *Newhard v. Borders*, 649 F. Supp. 2d 440 (W.D. Va. 2009); *United States v. Wurie*, 612 F. Supp. 2d 104 (D. Mass. 2009); *Brady v. Gonzalez*, 2009 WL 1952774 (N.D. Ill. July 2, 2009); *United States v. Quintana*, 594 F. Supp. 2d 1291 (M.D. Fla. 2009); *United States v. McCray*, 2009 WL 29607 (S.D. Ga. Jan. 5, 2009); *United States v. Gates*, 2008 U.S. Dist. Lexis 102989 (D. Me. Dec. 19, 2008); *United States v. Santillan*, 571 F. Supp. 2d 1093 (D. Ariz. 2008); *United States v. Deans*, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008); *United States v. Valdez*, 2008 WL 360548 (E.D. Wis. Feb. 8, 2008); *United States v. Curry*, 2008 U.S. Dist. LEXIS 5438 (D. Me. Jan. 23, 2008); *United States v. Dennis*, 2007 WL 3400500 (E.D. Ky. Nov. 13, 2007); *United States v. Lottie*, 2007 WL 4722439 (N.D. Ind. Oct. 12, 2007); *United States v. Mercado-Nova*, 486 F. Supp. 2d 1271 (D. Kan. 2007); *United States v. Zamora*, 2006 WL 418390 (N.D. Ga. 2006); *United States v. Murphy*, 2006 WL 3761384 (W.D. Va. 2006); *United States v. Diaz*, 2006 WL 3193770 (N.D. Cal. Nov. 2, 2006); *United States v. Cote*, 2005 WL 1323343 (N.D. Ill. May 26, 2006); *United States v. Brookes*, 2005 WL 1940124 (D. V.I. June 16, 2005); *United States v. Parada*, 289 F. Supp. 2d 1291 (D. Kan. 2003); *People v. Diaz*, 244 P.3d 501 (Cal. 2011); *Fawdry v. State*, 2011 WL 1815328 (Fla. App. 1 Dist. May 13, 2011); *Smallwood v. State*, 2011 WL 1599620 (Fla. App. Dist. 1 Apr. 29, 2011); *Hawkins v. State*, 704 S.E.2d 886 (Ga. App. 2010); *People v.*

## RONALD I. WEINER, PHD, LLC

*Specializing in Forensic Mental Health Services for over 40 years*

### ◆ SEX OFFENDER ASSESSMENT & TREATMENT SERVICES

COMPREHENSIVE PSYCHOSEXUAL RISK ASSESSMENT & TREATMENT PLANNING

### ◆ WHITE COLLAR CRIME/FRAUD FORENSIC SENTENCING EVALUATIONS

### ◆ DOMESTIC VIOLENCE ABUSER INTERVENTION PROGRAM

### ◆ SEXUAL ADDICTION/SEXUAL DISORDERS OUTPATIENT TREATMENT PROGRAM

### ◆ OTHER FORENSIC EVALUATIONS

WWW.RWEINERPHDLLC.COM

RONALD I. WEINER, PHD, LLC  
801 Roeder Road, Suite 950  
Silver Spring, MD 20910  
301-949-4907 ◆ 301-585-8740 (FAX)



*Shepard*, 2008 WL 4824083 (Cal. App. 6 Dist. Nov. 7, 2008); *State v. Harris*, 2008 WL 4368209 (Ariz. App. Div. 1 Sept. 23, 2008).

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

16. *Id.* at 259-60.

17. See *United States v. McGhee*, 2009 WL 242104 (D. Neb. July 21, 2009); *United States v. Wall*, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008); *United States v. Quintana*, 594 F. Supp. 2d 1291 (M.D. Fla. 2008); *United States v. Park*, 2007 WL 1521573 (N.D. Cal. May 23, 2007); *United States v. LaSalle*, 2007 WL 1390820 (D. Hawaii May 9, 2007); *Commonwealth v. Diaz*, 2009 WL 2963693 (Mass. Super. Ct. Sept. 3, 2009); *State v. Smith*, 920 N.E.2d 949 (Ohio 2009); *State v. Novicky*, 2008 WL 1747805 (Minn. App. Apr. 15, 2008). 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*, 2008 WL 1925032 (E.D. Mo. Apr. 29, 2008); *United States v. Carroll*, 2008 WL 313801 (N.D. Ga. Feb. 1, 2008). Finally, the Wisconsin Supreme Court recently rejected the warrantless search of the picture gallery of a cell phone 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*, 778 N.W.2d



1, 9-14 (Wis. 2010).

18. See *State v. Smith*, 920 N.E.2d 949 (Ohio 2009).

19. *Id.* at 954.

20. *Id.*

21. *Id.* at 955.

22. 2007 WL 1521573 (N.D. Cal. May 23, 2007).

23. *Id.* at \*8.

24. *Id.* at \*9.

25. See *United States v. McGhee*, 2009 WL 242104 (D. Neb. July 21, 2009); *United States v. Quintana*, 594 F. Supp. 2d 1291 (M.D. Fla. 2008).

26. *Gant*, 129 S. Ct. at 1719.

27. See *Commonwealth v. Diaz*, 2009 WL 2963693 (Mass. Super. Ct. Sept. 3, 2009).

28. *United States v. LaSalle*, 2007 WL 1390820 (D. Hawaii May 9, 2007).

29. *Id.* at \*6-8.

30. See *Belton*, 453 U.S. at 460-61.

31. See *id.* at 468 (Brennan, J., dissenting); *id.* at 472 (White, J., dissenting).

32. For contrary authority, see *State v. Stroud*, 720 P.2d 436, 439, 441 (Wash. 1986).

33. See *United States v. Nichols*, 512 F.3d 789, 797-98 (6th Cir. 2008); *United States v. Gonzalez*, 71 F.3d 819 (11th Cir. 1996); *United States v. Woody*, 55 F.3d 1257 (7th Cir. 1995); *United States v. McCrady*, 774 F.2d 868 (8th Cir. 1985); *People v. Perez*, 214 P.3d 502 (Col. Ct. App. 2009); *Hamel v. State*, 943 A.2d 686 (Md. Ct. Spec. App. 2008); *State v. Church*, 2008 WL 4947653 (Del. Super. Ct. Nov. 19, 2008); *People v. Dieppa*, 830 N.E.2d 870 (Ill. App. 3d 2005); *State v. Brooks*, 446 S.E.2d 579 (N.C. 1994); *State v. Hanna*, 839 P.2d 450 (Ariz. 1992); *State v. Farr*, 587 A.2d 1047 (Conn. App. 1991); *Lewis v. United States*, 632 A.2d 383 (D.C. App. 1989); *Staten v. United States*, 562 A.2d 90 (D.C. App. 1989); *State v. Gonzalez*, 507 So.2d 772 (Fla. Dist. Ct. App. 1987); *State v. Fry*, 388 N.E.2d 565 (Wis. 1986); *State v. Massenburg*, 310 S.E.2d 619 (N.C. App. 1984); *State v. Reed*, 634 S.W.2d 665 (Tenn. Crim. App. 1982); *Smith v. United States*, 435 A.2d 1066 (D.C. 1981).

34. See *United States v. Thomas*, 11 F.3d 620, 625, 628 (6th Cir. 1993).

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

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

37. See *United States v. Alvarado-Garcia*, 781 F.2d 422, 424, 427 (5th Cir. 1986); *Shaw v. State*, 449 So.2d 976 (Fla. App. 1 Dist. 1984).

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

39. 415 U.S. 800, 801 (1974).

40. 433 U.S. 1 (1977).

41. *Id.* at 16 n.10.

42. *Id.* at 15.

43. See *United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993); *United States v. McEachern*, 675 F.2d 618, 622 (4th Cir. 1982);

*United States v. Baldwin*, 644 F.2d 381, 384 (5th Cir. 1981); *United States v. Passaro*, 624 F.2d 938, 944 (9th Cir. 1980); *United States v. Castro*, 596 F.2d 674, 677 (5th Cir. 1979); *People v. Blankymsee*, 764 N.Y.S.2d 331, 334 (N.Y. Sup. 2003); *Roose v. State*, 759 P.2d 478 (Wyo. 1988); *State v. Rodewald*, 376 N.W.2d 416, 419 (Minn. 1985); *State v. Garcia*, 665 P.2d 1381 (Wash. App. 1983); *People v. Knight*, 333 N.W.2d 94 (Mich. App. 1983); *Chambers v. State*, 422 N.E.2d 1198, 1203 (Ind. 1981).

44. See, e.g., *United States v. Venizelos*, 495 F. Supp. 1277, 1283 (S.D.N.Y. 1980); *Preston v. State*, 784 A.2d 601, 608 (Md. App. 2001); *People v. Thomas*, 760 N.E.2d 1012 (Ill. App. Ct. 2001); *State v. Wade*, 573 N.W.2d 228 (Wis. App. 1997); *People v. Mannozi*, 632 N.E.2d 627, 632 (Ill. App. Ct. 1994); *State v. Greene*, 785 S.W.2d 574, 576 (Mo. App. 1990); *State v. Woods*, 637 S.W.2d 113, 116 (Mo. App. 1982); *People v. Harris*, 164 Cal. Rptr. 296 (Ct. App. 1980).

45. See *United States v. Morales*, 549 F. Supp. 217, 224 & n.5 (S.D.N.Y. 1982).

46. See *People v. Boff*, 766 P.2d 646, 651 & n.9 (Colo. 1988).

47. See *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007); *United States v. Wurie*, 612 F. Supp. 2d 104 (D. Mass. 2009); *United States v. Murphy*, 552 F.3d 405, 412 (4th Cir. 2009); *People v. Diaz*, 81 Cal. Rptr.3d 215, 217-18 (2008); *United States v. Curry*, 2008 U.S. Dist. LEXIS 5438, at \*24-27 (D. Me. Jan. 23, 2008); *United States v. Diaz*, 2006 WL 3193770 (N.D. Cal. Nov. 2, 2006), at \*4; see also *United States v. Lynch*, 908 F. Supp. 284, 289 (D. V.I. 1995) (involving a pager).

48. 477 F.3d 250 (5th Cir. 2007).

49. *Id.*

50. 2007 WL 1521573, at \*2 (N.D. Cal. May 23, 2007).

51. *Id.* at \*8.

52. *Id.*

53. See *Albert W. Alschuler, Bright-Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227, 281-82 (1984).

54. Compare *United States v. Weaver*, 433 F.3d 1104, 1106-07 & n.1 (9th Cir. 2006) (upholding search after 10- to 15-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 30 minutes after arrest); *State v. Hernandez*, 113 P.3d 437 (Or. App. 2005) (upholding search occurring 20 to 30 minutes after arrest); *United States v. Hrasky*, 453 F.3d 1099 (8th Cir. 2006) (upholding search occurring more than one hour after arrest, although over vigorous dissent) with *United States v. \$649,558 in United States Currency*, 955 F.2d 712, 716-17 & n.7 (D.C. Cir. 1992) (rejecting search incident to arrest doctrine for a search conducted between 30 and 63 minutes after arrest);

*United States v. Vasey*, 834 F.2d 782, 787-88 (9th Cir. 1987) (search of automobile 30 to 45 minutes after arrest was too long to be incident to arrest); *State v. Barksdale*, 540 A.2d 901, 907 (N.J. Super. 1988) (finding search more than 10 minutes after arrest to be "anything but a contemporaneous incident of that arrest").

55. See *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).

56. See, e.g., *People v. Landry*, 80 Cal. Rptr. 880 (Cal. App. 1969) (rejecting search occurring one hour and 15 minutes after arrest).

57. See *Ashlee Vance, If Your Password Is 123456, Just Make It HackMe*, N.Y. TIMES, Jan. 20, 2010.

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

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

60. See *Amber Hunt, Latest Police Weapon: iWitness*, USA TODAY, July 7, 2010, at 1.

61. See, e.g., *Removing iPhone 3G(s) Passcode and Encryption* (available at <http://www.youtube.com/watch?v=5wS3AMbXRLs>); *How to Bypass iPhone's Passcode* (available at <http://www.youtube.com/watch?v=OBUDSsp5U-4&feature=related>).

62. See ZDZIARSKI, *supra* note 59, at 19.

63. See *Miranda v. Arizona*, 366 U.S. 436 (1966).

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

65. 538 U.S. 760, 773 (2003) (plurality opinion). ■

## About the Author

Adam M. Gershowitz is an Associate



Professor at the University of Houston Law Center. He teaches and writes in the areas of criminal law and procedure.

### Adam Gershowitz

Associate Professor of Law  
University of Houston Law Center  
100 Law Center  
Houston, TX 77204  
713-743-0325

E-MAIL [amgersho@central.uh.edu](mailto:amgersho@central.uh.edu)