2011

Can a Password Stop Police from Searching Your Cell Phone Incident to Arrest?

Adam M. Gershowitz
William & Mary Law School, amgershowitz@wm.edu

SEARCH AND SEIZURE LAW REPORT

Vol. 38, No. 10 November 2011

Can a Password Stop Police From Searching Your Cell Phone Incident to Arrest?*

by Adam M. Gershowitz
Associate Professor of Law,
University of Houston Law Center

Over the last decade, cell phone use has exploded. Most Americans now use cell phones that contain huge amounts of information such as 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. Numerous defendants have been convicted of drug dealing, child pornography, and other offenses based on evidence found on their cell phones.

In an earlier article, Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27 (2008), 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. So long as police have a valid reason to arrest a suspect and find a cell phone on his person or immediately nearby, the search incident to arrest doctrine should permit police to search the arrestee's phone, even if there is no reason to believe the phone contains evidence related to the arrest. The only significant restriction on the search of cell phones incident to arrest is that the search must be conducted close in time, that is "contemporaneously," with the arrest.

Although it is far from a routine practice, the number of cell phone searches incident to arrest has risen dramatically recently. Over the last few years, more than fifty courts have been called upon to assess the constitutionality of searching cell phones incident to arrest. And the vast majority of those courts have approved of the practice.

With so little judicial protection against warrantless cell phone searches, this issue of SEARCH & SEIZURE LAW REPORT explores whether individuals can protect themselves 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 to answer. Under case law predating the internet, police are permitted to break into containers to search them incident to arrest. Courts have regularly upheld searches where police have unlocked or broken into locked glove compartments, briefcases, and even locked safes during searches incident to arrest. 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

*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).

WEST®

TABLE OF CONTENTS

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) that police can guess. And it should be worrisome to iPhone users whose devices have weak password protection functions that are vulnerable to tampering.

The second question – how long police can take in an effort to decipher or bypass the password – is more complicated. In an "ordinary" search incident to arrest, officers must conduct the search contemporaneous with arrest. Although there is no fixed time limit, courts require such searches to be conducted as soon as is practicable and rarely tolerate lengthy drawn-out searches. This limitation is deceiving in the context of cell phone searches however. Supreme Court precedent provides that when police conduct the search of 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 stationhouse rather than 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 that the police can take hours to try to break the password, including by using 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 their cell phones. In most cases, before requesting a cell phone password, police should be obligated to read the arrestee his *Miranda* rights. 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.

... 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

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," not situations where the police find no evidence and the individual is allowed to go on his way.

This issue of SEARCH & SEIZURE LAW REPORT 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. And because many Americans choose overly simplistic passwords and certain cell phones can easily be hacked, there is a chance that police can break into the phone without any help from the arrestee. If police were to 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 lead to the suppression of evidence. Only if police demand that an arrestee provide his password, can he make out a plausible (though still very weak) Fifth Amendment claim.

Supreme Court's "standard" search incident to arrest doctrine

The starting point for today's broad search incident to arrest doctrine is the Supreme Court's 1969 decision in *Chimel v. California*, 395 U.S. 752 (1969). In *Chimel*, the Court suppressed evidence found when police searched 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 *U.S. v. Robinson*, 414 U.S. 218 (1973), the Court moved a step further and clarified that police could open closed containers when searching incident to arrest. Police arrested 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 up 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 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 if the officers have no suspicion that the contents of the container are illegal. Put differently, the Court in *Robinson* clarified that the search incident to arrest doctrine is automatic and that courts should not conduct case-by-case inquiry to determine whether there was any suspicion or whether the search was truly necessary to protect the officer or prevent the destruction of evidence.

Searching cell phones incident to arrest

As wireless technology has become ubiquitous, 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-2000's 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. In many instances, police likely found nothing incriminating and in other cases defendants likely plead guilty without challenging the constitutionality of the searches. Nevertheless, more than fifty defendants have challenged the warrantless search of early generation cell phones over the last few years and courts have upheld the searches in the vast majority of cases. For instance, in *U.S. v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007), the court upheld a search of text messages because "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."

Dozens of other courts have reached the same conclusion. *See, e.g., People v. Diaz*, 244 P.2d 501 (Cal. 2011); *U.S. v. Pineda-Areola*, 2010 WL 1490369 (7th Cir. 2010); *U. S. v. Fuentes*, 2010 WL 724186 (11th Cir. 2010); *U.S. v. Murphy*, 552 F.3d 405 (4th Cir. 2009); *Silvan W. v. Briggs*, 2009 WL 159429 (10th Cir. 2009); *U. S. v. Faller*, 681 F.

SEARCH AND SEIZURE LAW REPORT

Coordinating Editor
John M. Burkoff

PUBLISHER'S STAFF
Darcie Bahr, *Attorney Editor*
Specialty Composition/Rochester DTP, *Electronic Composition*

Search and Seizure Law Report (USPS# pending) is issued monthly except in August, 11 times per year; published and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526 St. Paul, MN 55164-0526. Application to mail at Periodical rate is pending at St. Paul, MN. **POSTMASTER:** Send address changes to Search and Seizure Law Report, 610 Opperman Drive, P.O. Box 64526 St. Paul, MN 55164-1526.

Subscription: $857.52 for eleven issues

ISSN 0095-1005

Supp.2d 1028 (E.D. Mo. 2010); *Newhard v. Borders*, 649 F. Supp.2d 440 (W.D. Va. 2009); *U.S. v. Wurie*, 612 F. Supp.2d 104 (D. Mass. 2009); *Brady v. Gonzalez*, 2009 WL 1952774 (N.D. Ill. 2009); *U.S. v. Quintana*, 594 F. Supp.2d 1291 (M.D. Fla. 2009); *U.S. v. McCray*, 2009 WL 29607 (S.D. Ga. 2009); *U.S. v. Gates*, 2008 U.S. Dist. Lexis 102989 (D. Me. 2008); *State v. Harris*, 2008 WL 4368209 (Ariz. App. Div. 1 2008); *U.S. v. Santillan*, 571 F. Supp.2d 1093 (D. Ariz. 2008); *U.S. v. Deans*, 549 F. Supp.2d 1085, 1094 (D. Minn. 2008); *U.S. v. Valdez*, 2008 WL 360548 (E.D. Wis. 2008); *U. S. v. Curry*, 2008 U.S. Dist. LEXIS 5438 (D. Me. 2008); *U.S. v. Dennis*, 2007 WL 3400500 (E.D. Ky. 2007); *U.S. v. Lottie*, 2007 WL 4722439 (N.D. Ind. 2007); *U. S. v. Mercado-Nova*, 486 F. Supp. 2d 1271 (D. Kan. 2007); *U.S. v. Zamora*, 2006 WL 418390 (N.D. Ga. 2006); *U.S. v. Murphy*, 2006 WL 3761384 (W.D. Va. 2006); *U.S. v. Diaz*, 2006 WL 3193770 (N.D. Cal. 2006); *U.S. v. Cote*, 2005 WL 1323343 (N.D. Ill. 2006); *U.S. v. Brookes*, 2005 WL 1940124 (D. VI. 2005); *U.S. v. Parada*, 289 F. Supp. 2d 1291 (D. Kan. 2003).

Although the *Finley* decision has been cited repeatedly 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. For instance, in *State v. Smith*, 920 N.E2d 949 (Ohio 2009), the Ohio Supreme Court, in a closely divided opinion, refused to accept the crucial premise that cell phones are just like any other container that might hold other objects inside. 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."

Other courts have rejected the search incident to arrest of cell phones that occurred too long after arrest to be contemporaneous. *See, e.g., U.S. v. Park*, 2007 WL 1521573 (N.D. Cal. 2007); *U.S. v. LaSalle*, 2007 WL 1390820 (D. Hawaii 2007); *Commonwealth v. Diaz*, 2009 WL 2963693, (Mass. Super. Ct. 2009).

In sum, there are a growing number of instances in which police have searched cell phones incident to arrest. And while a few courts have rejected such searches on privacy and contemporaneousness grounds, the overwhelming majority of courts have upheld the searches. Because it is unclear whether the Supreme Court will step into this area of law and it is unlikely that legislatures will provide much statutory protection, it will be left to cell phone users themselves to protect against warrantless searches. The most plausible option is for cell phone users to password protect their phones.

Police can search locked containers incident to arrest

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. Yet, password protecting a phone does not cloak it in impenetrable Fourth Amendment protection. Password protecting a phone is equivalent to locking a closed container and lower courts have upheld the searches of locked containers.

... password protecting a phone does not cloak it in impenetrable Fourth Amendment protection

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*, 453 U.S. 454, 460-61 (1981), which authorized the search of the passenger compartment of a vehicle, broadly stated that police could search "any" containers, whether "open or closed." And the *Belton* dissenters clearly expressed their belief that the decision extended to locked containers. 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 they do not irreparably damage them.

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 held that police may open locked glove compartments during searches incident to arrest. *See, e.g., U.S. v. Nichols*, 512 F.3d 789, 797-98 (6th Cir. 2008); *U.S. v. Gonzalez*, 71 F.3d 819 (11th Cir. 1996); *U.S. v. Woody*, 55 F.3d 1257 (7th Cir. 1995); *U.S. v. McCrady*, 774 F.2d 868 (8th Cir. 1985); *People v. Perez*, 214 P.3d 502 (Col. App. 2009); *Hamel v. State*, 943 A.2d 686 (Md. Spec. App. 2008); *State v. Church*, 2008 WL4947653 (Del. Super. Ct 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. U.S.*, 562 A.2d 90 (D.C. App. 1989); *State v. Gonzalez*, 507 So.2d 772 (Fla. Dist. 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. U.S.*, 435 A.2d 1066 (D.C. 1981)

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 *U.S. v. Thomas*, 11 F.3d 620, 628 (11th Cir. 1993) the Sixth Circuit approved the search incident to arrest of a locked twenty-pound safe that was contained in a tote bag and found on the backseat of a pickup truck. Officers removed the car keys from the truck's ignition and found the key to the safe on the key ring. The court concluded that searching the safe fell squarely within the search incident to arrest doctrine.

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

Courts have likewise permitted police to search locked briefcases and overnight bags incident to arrest. One federal court even upheld the search incident to arrest when police pried open the latch of a locked briefcase with a screwdriver. *See U.S. v. Howe*, 313 F. Supp. 2d. 1178 (D. Utah 2003).

Courts have been less consistent in cases where police have tampered 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. Thus, courts have suppressed evidence where police have removed a vehicle seat or dismantled the tailgate when searching incident to arrest. *See* DAVID S. RUDSTEIN ET AL., CRIMINAL CONSTITUTIONAL LAW § 2.06[4][b] (2009). Yet, even in the face of this logical rule, a number of lower courts have given police leeway to conduct searches incident to arrest of sealed areas. For example, the Eighth Circuit upheld the search incident to arrest of the space between the window's rubber seal and the door panel. *See U.S. v. Barnes*, 374 F.3d 601, 604 (8th Cir. 2004).

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

Searching a locked (password protected) phone is permissible

Based on this caselaw, 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.

Of course, there is still a limit on the manner in which police can conduct the search incident to arrest. As with tangible objects like an automobile, police should be cabined by a rule forbidding them from destroying an object in order 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 times in a row. 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.

Attempts to break passwords must be contemporaneous with arrest

In ascertaining 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 *U.S. v. Edwards*, 415 U.S. 800 (1974), police arrested Edwards at 11pm for attempting to break into a government building. 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, ten 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 *U.S. v. Chadwick*, 433 U.S. 1 (1977), officers arrested Chadwick as he was trying to load a double-locked footlocker into his vehicle. One set of agents brought Chadwick to a federal building and another group of agents followed behind with the footlocker. Approximately ninety 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." 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."

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 person and are merely nearby, then there is a more rigid time limitation. In the three-and-a-half decades since *Edwards* and *Chadwick* have been decided, the Supreme Court has offered no additional guidance. There are, however, a few relatively clear principles that can be deciphered from lower court decisions.

Lower courts have repeatedly concluded that, in addition to clothing, police may also search wallets incident to arrest at the stationhouse. *See, e.g., U.S. v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993). Courts have concluded that wallets fall under *Edwards* because they are typically found on the arrestee and are thus much closer to a person's clothes than a footlocker. Similarly, courts have upheld stationhouse searches incident to arrest of purses, dufflebags, and backpacks because they appeared to more closely resemble items on the person rather than nearby possessions like the footlocker in *Chadwick*. As Professor Wayne LaFave has observed in his influential treatise, courts have "rather consistently" held that under *Edwards* police can search incident to arrest the "pockets, wallet, [and] other containers on the person" at the stationhouse following arrest. *See* 3 WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 5.3(a) at 146-47 (4th ed. 2004).

When a cell phone is found in an arrestee's pocket, precedent strongly suggests it should be treated like a wallet or any other item on the person that is searchable for hours after the arrest at the stationhouse under *Edwards*. A number of lower courts have reached this conclusion. *See U.S. v. Finley*, 477 F.3d 250 (5th Cir. 2007); *U.S. v. Murphy*, 552 F.3d 405, 412 (4th Cir. 2009); *U.S. v. Wurie*, 612 F. Supp. 2d 104 (D. Mass. 2009); *U.S. v. Curry*, 2008 U.S. Dist. LEXIS 5438, at *24-27 (D. Me. 2008); *U.S. v. Diaz*, 2006 WL 3193770 (N.D. Cal. 2006), at *4; *People v. Diaz*, 81 Cal.Rptr.3d 215, 217-18 (2008). *But see U.S. v. Park*, 2007 WL 1521573 (N.D. Cal. 2007) (concluding that cell phones should fall under Chadwick because they contain an enormous amount of information).

If cell phones are merely possessions, how long can police spend searching them before the search ceases to be contemporaneous?

If a court rejects the contention that the phone falls under *Edwards* and instead finds *Chadwick* controlling, police will have far less time to search it incident to arrest. 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 searches under Chadwick. Not surprisingly, lower court decisions often appear to be completely inconsistent with one another.

While courts have refused to draw bright line time limits on searches incident to arrest, the contours of the caselaw does suggest that there is an outer time limit. 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. *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). But very few cases involve searches more than an hour after arrest. *See, e.g., People v. Landry*, 80 Cal. Rptr. 880 (Cal. App. 1969) (rejecting search occurring one hour and fifteen minutes after arrest). 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 lying 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.

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. While some people use overly simple passwords such as "12345" that police can guess, in most cases, police simply will not be able to decipher the password during the commotion of an arrest.

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 ten times. Unfortunately, these protections are extremely weak.

A four digit numerical code provides only ten thousand 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 ten thousand 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 a password, they may be able to bypass the password altogether by hacking into the phone. Numerous internet videos that show users how to access the data on the iPhone. 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. 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 Fifth Amendment

As detailed above, 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 the password to the police?

As explained 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 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 can fail to comply with *Miranda* and suffer no consequences.

If arrestees turn over their password in response to a police demand (as opposed to a voluntary request), the arrestee can make only a very 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.

Miranda doctrine may protect against requests for passwords, but violations will not lead to suppression of valuable evidence

For the *Miranda* doctrine to apply, an individual must be in custody and subject to interrogation. The interrogation element is easily satisfied. When a police officer asks an individual "What is your password?," that inquiry is a question that constitutes interrogation. 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 interrogation if they are designed to elicit an incriminating response. Accordingly, requesting that an arrestee voluntarily turn over the password to his phone (which may inculpate him by leading to evidence on the phone) amounts to interrogation.

The custody question is also fairly simple. 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, it seems clear that an individual who has been formally subjected to a full-scale custodial arrest is in custody for *Miranda* purposes. 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.

Yet, as in many other instances, the *Miranda* requirement is a hollow protection, because the fruit of the poisonous tree doctrine does not apply to *Miranda* violations. *See Oregon v. Elstad*, 470 U.S. 298 (1985). 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 inadmissible, but the valuable resulting evidence – the incriminating text messages or child pornography found on the phone – will be admissible.

Police demands for password likely do not amount to violation of Fifth Amendment's self-incrimination clause

A final problem worthy of attention is what happens if police demand (rather than request) that the 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."

In order to assert a Fifth Amendment self-incrimination challenge, an individual must demonstrate three things: (1) that he has been compelled; (2) to produce testimony; (3) that is incriminating. 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 the 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." *Hoffman v. U.S.*, 341 U.S. 479, 486 (1951). Thus, if providing the password leads to incriminating information, the element is satisfied.

It is also fairly easy to satisfy the "testimonial element. Evidence is testimonial (and thus protected by the Fifth

Amendment) if it causes a person "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." *Doe v. U.S.*, 487 U.S. 201, 213 (1988). 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."

While the incriminating and testimonial elements are 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 cases in which defendants have been compelled to disclose their computer passwords have been in response to grand jury subpoenas. *See U.S. v. Kirschner*, 2010 WL 1257355 (E.D. Mich. 2010); *In re Boucher*, 2009 WL 424718 (D. Vt. 2009).

The idea that police cannot compel incriminating testimony is further supported by the Supreme Court's plurality decision in *Chavez v. Martinez*, 538 U.S. 760 (2003). 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 no criminal charges had ever been filed against him and therefore he had not been forced to incriminate himself in a criminal case in violation of the Fifth Amendment. 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 Amendment's due process clauses, not the Self-Incrimination Clause.

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.

Moreover, even if the self-incrimination claim were viable, most arrestees will never be in a position to assert it because they will have revealed the password voluntarily. If police simply ask, rather than demand, that an arrestee consensually enter the password to his phone, there will have been no compulsion and hence no Fifth Amendment violation. At bottom, arrestees likely have little or no self-incrimination protection against police demands for cell phone passwords.

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 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.

... password protecting the phone provides virtually no additional protection against police searching a cell phone incident to arrest

Moreover, even if police cannot decipher the password on their own, they stand a strong chance of acquiring the password from simple police interrogation. Requesting the password would require police to give *Miranda* warnings, yet most individuals waive their *Miranda* rights and, in any event, violations of *Miranda* do not lead to suppression of evidence found subsequently. Arrestees would 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.

In sum, police 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 police power to search digital devices incident to arrest.