Searching Cell Phones Incident to Arrest: Can Courts and Legislatures Impose Limits on a Bright Line Rule?

Adam M. Gershowitz

William & Mary Law School, amgershowitz@wm.edu
Imagine that Defendant Dan is stopped by the police for driving through a stop sign. The officer thinks that Dan looks suspicious, but has no probable cause to believe Dan has done anything illegal, other than driving recklessly. Because running a stop sign is an arrestable offense and the officer is suspicious that Dan might be involved in more serious criminal activity, the officer arrests Dan for the traffic violation.

Under the search incident to arrest doctrine, officers are entitled to search the body of the arrestee to ensure that he does not have weapons and to prevent him from destroying evidence. The search incident to arrest is automatic and allows officers to open containers found on the person, even when there is no probable cause to believe anything illegal is inside. For instance, a standard search incident to arrest often turns up drugs located in a small container such as a cigarette pack. Yet, Dan does not have a cigarette pack in his pocket; instead, like millions of other technophiles, Dan is carrying an iPhone.

The officer removes the iPhone from Dan's pocket and begins to rummage through Dan's cell phone contacts, call history, emails, pictures, movies, and, perhaps most significantly, his internet browsing history. Thus, in addition to finding Dan's personal financial data and embarrassing personal information, the police also discover incriminating pictures of stolen contraband, emails evidencing drug transactions, and internet surfing of websites containing child pornography. Is all of this evidence admissible even though Dan has only been arrested for a traffic infraction and there was no probable cause to search the contents of his iPhone? When one considers the breadth of information located in Dan's iPhone, it would seem shocking that officers need no suspicion whatsoever in order to search through that information. Yet, that result appears to follow from longstanding U.S. Supreme Court precedent laid down well before handheld technology was even contemplated.

...if we think of an iPhone as a container—like a cigarette package or a closed box—police can open and search the contents inside with no questions asked and no probable cause required, so long as they are doing so pursuant to a valid arrest.

For nearly four decades, the search incident to arrest doctrine has functioned as a bright-line rule—allowing police to search the entire person of an arrestee without getting into sticky questions of whether there was probable cause to open a particular container. See U.S. v. Robinson, 414 U.S. 218, 235 (1973). While society and technology have changed drastically over the last few decades, the search incident to arrest rule has remained static. Thus, if we think of an iPhone as a container—like a cigarette package or a closed box—police can open and search the contents inside with no questions asked and no probable cause required, so long as they are doing so pursuant to a valid arrest. And as scholars have long recognized, states have expansive criminal codes that give
Search incident to arrest doctrine as a search for bright-line rules
Bright-line rules in an era of pagers and cell phones
Stakes and likely results when iPhone meets search incident to arrest doctrine
Disentangling iPhone from bright-line rule: possible approaches to cabining search incident to arrest doctrine
Change nothing: Search incident to arrest rule works well, so changing it to account for new technology is not good idea
Change everything: Limiting search incident to arrest doctrine in all police interactions to search related to crime of arrest
Change different sovereign: Encouraging state legislatures to adopt more protective rule
Change at the margins: Open application test
Changing bright-line rule: Limiting search incident to arrest doctrine to five steps of searches
Distinguishing between data on device and remotely-stored data accessible from device
Conclusion

police authority to arrest for a huge number of infractions. Thus, police officers with nothing more than a bunch of illegal activity may arrest an individual for a simple traffic violation, Atwater v. City of Lago Vista, 532 U.S. 318 (2001), and proceed to search thousands of pages of private data located on the iPhone found in an arrestee’s pocket.

This issue of Search & Seizure Law Report provides an overview of the history and scope of the search incident to arrest exception to the warrant requirement. It then explains the complicated problems that develop when this doctrine is applied to iPhones and other advanced cell phones. It also offers a number of approaches that courts and legislatures could adopt to narrow the scope of warrantless searches of iPhones and similar handheld wireless devices.

Search incident to arrest doctrine as a search for bright-line rules
The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause.” Yet, as any criminal procedure student knows, the Supreme Court has long recognized a slew of exceptions allowing the police to search without first procuring a warrant. There is one exception of particular significance, perhaps the most common rationale for police to search without a warrant—the search incident to arrest doctrine.

The history of the search incident to arrest exception dates back to the creation of the exclusionary rule in 1914, when the Supreme Court obligingly suggested in dictum that the government has the right “to search the person of the accused when legally arrested, to discover and seize the fruits or evidences of crime.” Weeks v. U.S., 232 U.S. 383, 392 (1914). Although the Court alluded to such searches in that case and a handful of other early decisions, the doctrine’s modern conception was the 1969 decision in Chimel v. California, 395 U.S. 752 (1969).

In Chimel, police arrested a suspect in his home for burglary and proceeded to search the entire three-bedroom house, as well as the attic and garage, for proceeds of that burglary. While the Court found this warrantless search to be unconstitutionally broad, it nevertheless recognized that police can search suspects incident to arrest in narrower circumstances. The Court explained that a search incident to arrest must be limited to a search for weapons that an arrestee could use against the officer and to prevent an arrestee from concealing or destroying evidence. The Court concluded that a search for weapons and evidence must be limited to the arrestee’s person and the area within his immediate control from which he might gain possession of a weapon or destroy evidence. The Court specifically rejected the contention that police could search areas beyond that from which an arrestee could grab a weapon or evidence.

A few years after Chimel, the Supreme Court addressed the question of whether police could open closed containers located on an arrestee’s person. In U.S. v. Robinson, 414 U.S. 218 (1973), police arrested a suspect for operating a motor vehicle with a revoked license. While conducting a search incident to arrest, the officer felt an object in Robinson’s coat pocket but could not tell what it was. The officer reached into the pocket and pulled out a “crumpled up cigarette package.” Still not sure what was in the package, the officer opened it and discovered capsules of heroin. In rejecting Robinson’s challenge to the search, the Court made clear that officers conducting a search incident to arrest can 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. The Court explained that the search incident to arrest doctrine does not require case-by-case adjudication and that there need not be analysis of each step of the search to determine whether it was necessary to prevent the arrestee from acquiring weapons or destroying evidence. Rather, Robinson made clear that searches of the arrestee’s person and the containers thereon can be conducted automatically incident to an arrest. The Court’s decision thus created a bright-line rule.

The Court’s affinity for bright-line rules became even clearer eight years later in New York v. Belton, 453 U.S. 454 (1981). In Belton, the officer stopped a car for speeding and, upon smelling marijuana, arrested the occupants. With the occupants away from the vehicle, the officer then searched the passenger compartment of the car and found a jacket in the backseat. The officer unzipped the pockets of the jacket and found cocaine. Praising its decision in Robinson, the Court reaffirmed that police officers must be afforded “a straightforward rule, easily applied, and predictably enforced.” Lamenting that there was not yet such a straightforward rule for the search of the interior of a car at a traffic stop, the Court adopted another bright-line rule permitting the search of the entire passenger compartment of an automobile when an occupant of the car is lawfully arrested.
Just as in Robinson, the Court made clear that the bright-line rule would apply even if there were no chance that an arrestee could break free of his restraints to grab a weapon or destroy evidence in the passenger compartment of the car. The Court further explained that the search of the passenger compartment included any containers found therein, whether open or closed, and irrespective of whether they could contain a weapon or evidence. The Belton decision marked a considerable expansion of the search incident to arrest doctrine.

In the Court’s last significant search incident to arrest decision, Thornton v. U.S., 541 U.S. 615 (2004), an automobile was again the focus of attention. Unlike the occupant in Belton, the Thornton case involved a driver who had already exited and walked away from his vehicle before being approached by police. After Thornton was arrested for drug possession, the officer then proceeded to his vehicle and searched the passenger compartment incident to arrest. The officer found a handgun under the seat, which led to a charge of possessing a firearm in furtherance of a drug-trafficking crime. The Court once again stressed the need for a “clear rule, readily understood by police officers and not depending on differing estimates of what items were or were not within reach of an arrestee at any particular moment.” In rejecting Thornton’s suppression argument, the Court extended the Belton rule to permit a full-scale search of the passenger compartment of a vehicle incident to the arrest of a “recent occupant” of a vehicle.

The Court’s decisions over the last forty years suggest that the search incident to arrest exception to the warrant requirement should be interpreted expansively. Indeed, in Belton, the Court specifically stated that “container” should be interpreted broadly to include “any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like.” Consistent with this guidance, lower courts have taken a broad approach and upheld searches of numerous small containers incident to arrest, such as wallets, U.S. v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993), envelopes, U.S. v. McCrady, 774 F.2d 868, 872 (8th Cir. 1985), and aspirin bottles, Daniels v. State, 416 So.2d 760 (Ala. Crim. App. 1982). Although some state courts have interpreted their own constitutions and criminal codes to be more restrictive than the U.S. Constitution, most lower courts have not hesitated to apply the search incident to arrest doctrine to new situations unforeseen by the Supreme Court.

Bright-line rules in an era of pagers and cell phones

The Supreme Court’s decisions in Robinson and Belton made clear that, incident to a lawful arrest, officers can open containers located on a person or in their immediate grabbing space without having any independent probable cause to search those containers. For many years, the only evidence found as a result of such searches was tangible physical evidence, such as drugs or illegal weapons. As technology has advanced however, lower courts have been forced to rule on the admissibility of nontangible digital evidence located in electronic devices, specifically pagers, cell phones, and computers. These courts have been forced to confront whether the search incident to arrest doctrine—designed with a world of tangible evidence in mind—should apply to data digitally contained in electronic devices. Most courts have upheld such searches.

The earliest of these electronic data cases (and consequently the most primitive of the technology at issue) was a 1993 decision from the Northern District of California dealing with a pager found on an arrestee. U.S. v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993). The defendant, Chan, was arrested as part of a drug sting operation and police found a pager on Chan’s person. The police then activated the pager’s memory function and retrieved telephone numbers stored inside it. Two numbers found in the pager linked Chan to the drug sting the police were conducting. Chan contended that he had a reasonable expectation of privacy in the pager and that activating it amounted to a search that required a warrant.

The court sided with Chan in part by agreeing that a pager is analogous to a closed container and that individuals have a reasonable expectation of privacy in the contents of electronic containers. However, the court ultimately concluded that because the search of the pager came on the heels of a lawful arrest of Chan, a warrantless search was permitted under the search incident to arrest doctrine. Citing Belton and Chimel, the court concluded that all containers can be searched incident to a lawful arrest, including electronic containers. Moreover, the court considered and specifically rejected as irrelevant the fact that Chan could not retrieve a weapon from the pager nor plausibly destroy any evidence from the pager. Accordingly, the evidence found when the officer turned on and searched the pager was admissible.

Over the next few years, a handful of other courts were called upon to analyze the question raised in Chan and these courts likewise permitted the search of the contents of a pager incident to arrest. See U.S. v. Hunter, 1998 WL 887280, at *3 (4th Cir. Oct. 29, 1998) (per curiam); U.S. v. Ortiz, 84 F.3d 977, 983–84 (7th Cir. 1996); U.S. v. Sirota, 1994 WL 711908, at *2 (9th Cir. Dec. 21, 1994); U.S. v. DiaZ-Lizaraza, 981 F.2d 1216, 1223 (11th Cir. 1993); U.S. v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996); U.S. v. Lynch, 908 F. Supp. 284, 290 (D.V.I. 1995).

The era of pagers has all but ended, making way for the age of cell phones. To date, approximately two dozen courts have addressed searches of cell phones incident to arrest. The Fifth Circuit’s recent decision in U.S. v. Finley, 477 F.3d 250 (5th Cir. 2007) is representative. Police arrested Finley after a staged drug sale. The police then searched Finley incident to arrest and found a cell phone in his pocket. One of the investigating officers searched through the phone’s records and found text messages that appeared to relate to drug trafficking. One incoming text message
sages or call logs as he could tear up a letter or an incriminating
sages, can easily
envelope, Much as the traditional search incident to arrest cases
makes sense to allow the police to review electronic call histories
12
search took place too long after the arrest to be considered a con­
in order to preserve it for use at trial.” The court further explained
that police can open containers found on the arrestee’s person and
saw no reason why the doctrine should not be extended to text
messages contained in a cell phone.
In short, the Fifth Circuit did not recognize any conceptual
difference between searching a person’s body or physical containers
on that body for drugs and searching electronic equipment for dig­
ital information. As of December 2008, nearly twenty other courts
have reached the same conclusion as the Fifth Circuit and ad­
nounced evidence seized from cell phones incident to arrest. See People
July 25, 2008); People v. Diaz, 81 Cal. Rptr. 3d 215, 219 (Cal.
App. 2 Dist. 2008); U.S. v. Santillan, 571 F. Supp. 2d 1093, 1102­
03 (D. Ariz. 2008); U.S. v. Young, 278 Fed. Appx. 242, 245-46
(4th Cir. May 15, 2008); U.S. v. Deans, 549 F. Supp. 2d 1085, 1094
(D. Minn. 2008); U.S. v. Valdez, 2008 WL 3605438, at *3 (E.D.
Wis. Feb. 8, 2008); U.S. v. Carrol, 357 F. Supp. 2d 1290, 1301-02
(N.D. Ga. 2008); U.S. v. Curry, 2008 WL 219966, at *8-10 (D.
Ind. Oct. 12, 2007); U.S. v. Mercado-Nava, 486 F. Supp. 2d 1271,
1275-76 (D. Kan. 2007); U.S. v. Murphy, 2006 WL 3761384, at
*4-5 (N.D. Cal. Nov. 2, 2006); U.S. v. Zamora, 2006 WL 418390,
*6 (D.N.H. May 26, 2005); U.S. v. Brookes, 2005 WL 1940124, at
*3 (D.V.I. June 16, 2005); U.S. v. Parada, 289 F. Supp. 2d 1291,
To be sure, two lower courts have suppressed evidence found
on cell phones pursuant to a search incident to arrest. See U.S. v.
Park, 2007 WL 1521573, at *11-12 (N.D. Cal. May 23, 2007); U.S.
v. Lasalle, 2007 WL 1390820, at *7-8 (D. Haw. May 9, 2007). Yet,
those decisions rested primarily on grounds that the search took place too long after the arrest to be considered a con­
temporaneous search incident to arrest.
Perhaps the reason for the lack of contrary authority is that
searching a conventional cell phone or pager incident to arrest
is relatively easy to square with precedent that permits police to
search tangible containers found on an arrestee. A cell phone’s
memory of incoming and outgoing calls, as well as its text mes­
ges, can easily be analogized to an address book or a letter in an
envelope. Much as the traditional search incident to arrest cases
permit police to open a wallet, take out a letter, and read it be­
fore the arrestee has an opportunity to destroy the evidence, it also
makes sense to allow the police to review electronic call histories
and text messages in a cell phone. An arrestee familiar with the
functions of his cell phone could just as easily delete text mes­
ges or call logs as he could tear up a letter or an incriminating
list of addresses on a piece of paper.

Stakes and likely results when iPhone
meets search incident to arrest
document

To date, no court has been called upon to address the constitu­tionality of searching an iPhone. In light of the handful of cell
phone and pager cases discussed by the lower federal and state
courts, it might seem that there is no difference in searching an
iPhone. Just as text messages stored on a cell phone are evidence
within a digital container, it would seem that call histories, emails,
and pictures on an iPhone would simply be characterized as evi­
dence stored in a (larger) digital container. As a conceptual mat­
ter, there is no real difference between a crumpled up cigarette
package, an early-generation cell phone, and an iPhone with a
much larger memory. Yet, this is cause for concern because no
matter what theoretical similarities exist between an iPhone and
a conventional cell phone (or a cigarette package for that matter),
the former stores tremendously more information in a very
different way. The differences can be demonstrated by thinking
about how many steps or searches police might be able to take
with respect to the new and old technology.
The cell phone and pager cases decided by courts in the last few
years are what we might call first level cases because they do not
require in-depth searching to obtain evidence. Police need to push
only a limited number of buttons in order to reach pager numbers
and only a few additional buttons to retrieve text messages. If we
think of each step that police must take to retrieve information as
a separate search, then reviewing pager numbers might amount to
only two levels of searches: first, pushing the memory button
for the list of recent pages; and second, scrolling through the
numbers to find the incriminating calls. Reviewing text messages on a
phone can be conceptualized as three separate searches: (1) open­ing
the text message function; (2) opening the list of received text
messages; and (3) opening and reading a particular text message.
This is similar to the searches in Robinson where the police officer
(1) felt the cigarette package; (2) pulled out the package; and (3)
opened the package.
Put simply, the data on early-generation cell phones is limited
in its amount and usefulness, and police officers will either find
the evidence or run into a dead end rather quickly. Accordingly,
the degree of privacy invasion can be measured by the number of
steps an officer must take to retrieve the incriminating informa­tion.
In the cases decided to date dealing with text messages and
pages, this number has been small because those devices have
few, relatively simple functions capable of storing electronic data.
The same can be said for tangible evidence such as cigarette
packages, purses, wallets, or suitcases.

...the iPhone stores tremendously
more information...

The iPhone drastically changes this situation for two reasons.
First, the iPhone stores tremendously more information —thereby
providing law enforcement with access to information that the
typical arrestee would otherwise be incapable of carrying in his
pocket. In addition to the text messages, contact information, and
call histories found on conventional phones, iPhones also contain
an iPhoto application. This application holds far more pictures
than could be stored on a conventional cell phone and displays
them in much clearer detail. Similarly, the iPhone’s easily acces­sible
email application makes it simple to access thousands of new,
saved, and sent email messages. The iPhone enables users to
store thousands of audio and video files. Music, books, and videos ranging from classical music to potentially obscene pornographic videos can be accessed with the touch of a few buttons.

Second, and perhaps with greater ramifications than the data stored on the actual device, the iPhone provides a mechanism for accessing information via the internet. The iPhone’s internet browser is just like the one found on a standard computer; it can dial out and retrieve information stored remotely with an internet service provider. An example is instructive.

Imagine that an officer arrests an individual following a lawful traffic stop and finds an iPhone in the driver’s pocket. The officer then takes the following steps: (1) activates the touch screen to view the phone’s contents; (2) clicks on the internet browser icon; (3) clicks on the toolbar to find the bookmarks link; (4) finds a suspicious-looking bookmark labeled “porn pictures”; (5) clicks on that particular bookmark to bring up the webpage; (6) sees that the webpage contains a series of icons including a “members” button and clicks on that image; (7) brings up the “members” page which has a saved account number and password already entered; (8) clicks on the “submit” button which utilizes the saved account information and password to bring up the content of the website; (9) sees that, in addition to pictures, the website also has a message function and the account owner has two new messages; and (10) clicks on the message icon and brings up the two new messages, both of which detail an intimidating conversation about exchanging pictures of underage children.

Or imagine how an officer could utilize the internet to circumvent an arrestee’s privacy protections, such as if an arrestee had password-protected his iPhone application to hide his photographs. After (1) turning on the iPhone; and (2) attempting to open the iPhone application, the officer discovers that the application is password-protected and cannot be opened. The officer might then (3) activate the internet browser; (4) click on the browsing history to see what webpages the owner had visited; (5) click on the history link that referenced the arrestee’s web-based email account—for instance, Yahoo! or Gmail; (6) read through the folders in the email account until finding one labeled “personal information”; (7) read through the messages in that folder until finding an email with the subject “passwords”; (8) open that email and retrieve the password for the iPhone application; (9) close the internet browser and again click on the iPhone application; (10) enter the password found in the email, thus opening the iPhone application; (11) search through the folders in the iPhone application, finding the most suspiciously labeled folder—for instance, “kid pics”; and (12) open that folder and search through all of the pictures inside that folder.

Countless other complicated scenarios could likewise be envisioned. As the scenarios become more convoluted, it becomes harder to analogize them to a closed container or a wallet containing an address list. And indeed, the iPhone provides access to information and password to bring up the content of the website; (9) sees that, in addition to pictures, the website also has a message function and the account owner has two new messages; and (10) clicks on the message icon and brings up the two new messages, both of which detail an intimidating conversation about exchanging pictures of underage children.

Or imagine how an officer could utilize the internet to circumvent an arrestee’s privacy protections, such as if an arrestee had password-protected his iPhone application to hide his photographs. After (1) turning on the iPhone; and (2) attempting to open the iPhone application, the officer discovers that the application is password-protected and cannot be opened. The officer might then (3) activate the internet browser; (4) click on the browsing history to see what webpages the owner had visited; (5) click on the history link that referenced the arrestee’s web-based email account—for instance, Yahoo! or Gmail; (6) read through the folders in the email account until finding one labeled “personal information”; (7) read through the messages in that folder until finding an email with the subject “passwords”; (8) open that email and retrieve the password for the iPhone application; (9) close the internet browser and again click on the iPhone application; (10) enter the password found in the email, thus opening the iPhone application; (11) search through the folders in the iPhone application, finding the most suspiciously labeled folder—for instance, “kid pics”; and (12) open that folder and search through all of the pictures inside that folder.

Disentangling iPhone from bright-line rule: possible approaches to cabining search incident to arrest doctrine

The difference between the data found on a cell phone and an iPhone is dramatic but, at present, the Fourth Amendment and its search incident to arrest doctrine make no distinction. Below, I offer approaches that courts and legislatures might adopt to address the problem.

Change nothing: search incident to arrest rule works well, so changing it to account for new technology is not good idea

While it is undoubtedly troubling to permit suspicionless searches of the many applications of an iPhone, one could plausibly argue that attempting to craft a rule disallowing such searches would be worse. At present, the search incident to arrest doctrine is a bright-line rule that is easy for police officers to understand and apply. And courts faced with a search incident to arrest usually have an easy time determining whether the officers’ actions were permissible. Compare this to the rest of Fourth Amendment law, which is riddled with exceptions, caveats, and uncertainty. Indeed, the typical Fourth Amendment section of a criminal procedure textbook is at least twice as long as the Fifth Amendment section. Carving out an exception to the search incident to arrest doctrine to deal with the iPhone might afford more privacy protection to a device that is capable of holding reams of personal information that individuals reasonably expect to be protected against government intrusion, but at what cost? There is a colorable argument that any benefit to be had from a new rule would be outweighed by muddling one of the few areas of Fourth Amendment law that is currently intelligible.

Nevertheless, while I do not desire that Fourth Amendment law be made any more complicated, ultimately, I am not convinced that courts should restrain themselves by applying an ill-fitting bright-line rule to the iPhone. I see two primary reasons.

First, the major informal constraints typically facing police in executing searches are not present with respect to the iPhone. Po-
lice investigations are ordinarily constrained by limited resources and limited time. For example, while the Supreme Court has held that there is no Fourth Amendment search when police observe backyards from helicopters or planes, Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion); California v. Ciraolo, 476 U.S. 207 (1986), that has not enabled police to do so with impunity. Police departments typically cannot afford to buy or rent helicopters, nor do they have the time to file flight plans, spend hours in the air, and simply look around without being guided by some particularized suspicion.

The iPhone drastically changes the amount of private information that can be accessed during a search incident to arrest.

With respect to the iPhone, however, the new technology inverts the typical state of affairs because it is the individual, not the police officer, who has the new technology. Moreover, unlike flyovers, the technology is everywhere. Apple is expected to sell more than ten million iPhones by the end of 2008. In the next decade, millions of drivers will have an iPhone or a substantially similar device in their pockets during many of the nearly thirty million traffic stops that occur each year. And unlike helicopters or airplane flyovers, the cost to police in searching is almost nil. A study by the Bureau of Justice Statistics found that police searched the car or the driver in 6.6 percent of the twenty-seven million traffic stops that occurred in a particular year. Upwards of 470,000 searches were conducted incident to arrest at a traffic stop. See BUREAU OF JUSTICE STATISTICS, U.S. DEPT OF JUSTICE, CHARACTERISTICS OF DRIVERS STOPPED (2002).

The iPhone drastically changes the amount of private information that can be accessed during a search incident to arrest. Because the stakes are higher and potentially could affect millions of individuals, it is worth considering whether the search incident to arrest doctrine might be amended to fix this problem.

Change everything: limiting search incident to arrest doctrine in all police interactions to search related to crime of arrest

The most drastic change to the search incident to arrest doctrine—short of abolishing it altogether—would be to limit officers to searching for evidence of the crime for which the suspect was arrested. Thus, if the driver were arrested for drug possession, police could search anywhere drugs might be found. But if the driver were arrested for failure to wear a seatbelt, a search for drugs would be impermissible. Justice Antonin Scalia advocated this revision to the search incident to arrest doctrine in his 2004 concurring opinion in Thornton v. U.S., in which the Supreme Court upheld the search of the passenger compartment of a "recently" occupied car. Joined by Justice Ruth Bader Ginsburg, Justice Scalia argued that searching a vehicle incident to arrest should only be permitted when "it is reasonable to believe evidence related to the crime of arrest might be found in the vehicle." Justice Scalia's view departs from the traditional rationale for the search incident to arrest doctrine. Instead of conducting the searches to prevent the arrestee from harming the officer or destroying evidence, such searches would be justified as "evidence-gathering" exercises that can be conducted because of "a reasonable belief that evidence [will] be found."

Justice Scalia wrote for only himself and Justice Ginsburg in expressing this view, so we might be inclined to dismiss this approach as simply unlikely to be adopted. However, it is not altogether implausible to assume that Justice Scalia's position may have some day command a majority: Chief Justice Roberts and Justice Alito have not yet had a chance to address this approach, and Justice Stevens and Justice Souter are on record as being very dissatisfied with the current state of the search incident to arrest doctrine.

Besides its unlikely adoption, perhaps a stronger objection to Justice Scalia's approach is that the evidence-gathering approach lacks doctrinal justification. Searching to gather evidence during a search incident to arrest is troubling because it would permit searches based on suspicion—rather than officer safety—that involve less than probable cause. Likewise, such an approach would offer no justification for permitting searches of the passenger compartment incident to arrest but not the trunk of the vehicle.

On the plus side, Justice Scalia's approach would solve the iPhone dilemma by reconceptualizing the entire search incident to arrest doctrine, without requiring a special rule for particular new technology. If police could only search for evidence related to the crime of arrest, most traffic stops would not permit searches of an iPhone's contents. And even when police were permitted to search an iPhone incident to arrest, the scope of the search would be limited. If an officer arrested a driver for possession of drugs with intent to distribute, it would make sense to search his text messages for further evidence of the crime, since that function is commonly used in conjunction with drug sales. But it would not seem to be permissible for the officer to search through the arrestee's pictures under the iPhone function or the history section under his internet browser because such applications likely have nothing to do with drug sales. A rule limiting the search incident to arrest exception to the crime of arrest would prevent police from roaming at large among the thousands of pages of data held in the iPhone.

Change by different sovereign: encouraging state legislatures to adopt more protective rule

Scholars dispute the ability of state courts to provide greater protection of constitutional rights than federal courts. Although the debate rages, it is undisputed that, in the criminal procedure context, a number of states have imposed greater restrictions on searches and seizures under their state constitutions. Notably, numerous state courts have caved the search incident to arrest exception under state law to narrower circumstances than authorized by the Supreme Court.

One approach states courts might take is the one advocated by Justice Scalia. If the Supreme Court refuses to limit the search incident to arrest doctrine to searches of the arrestee for weapons and evidence of the crime for which he has been arrested, then the state courts could look to their own constitutions to do so. To date, a handful of state courts have adopted this approach. State v. Ringer, 674 P.2d 1240 (Wash. 1983) (en banc); State v. Caraher, 653 P.2d 942 (Or. 1982) (en banc).

Moreover, we should look beyond state courts to consider the role of state legislatures in crafting statutory protections. While new criminal procedure rules typically come from courts, it would be a mistake to ignore possible legislative solutions. And, indeed,
legislatures have taken action in the past to narrow what they believe to be an overly broad search incident to arrest doctrine.

In the wake of the Supreme Court's expansive 1973 decision in U.S. v. Robinson permitting police to open all containers on a person incident to a lawful arrest, the Massachusetts legislature adopted statutory language specifically designed to narrow the search incident to arrest doctrine. For over thirty years, that statute has provided that:

[a] search conducted incident to an arrest may be made only for the purposes of seizing fruits, instrumentalities, contraband and other evidence of the crime for which the arrest has been made, in order to prevent its destruction or concealment; and removing any weapons that the arrestee might use to resist arrest or effect his escape. Property seized as a result of a search in violation of the provisions of this paragraph shall not be admissible in evidence in criminal proceedings.

MASS. GEN. LAWS ANN. ch. 276, § 1 (West 2004).

Other state legislatures could revise their codes to follow the Massachusetts model. Or those legislatures could take a different approach and authorize the seizure of iPhones or other wireless devices incident to arrest but prohibit warrantless searches of those devices without a warrant.

The key question is, how likely are legislatures to take action to protect iPhones from warrantless searches? Legislatures are not typically in the business of limiting police officers' ability to conduct criminal investigations. To the contrary, legislators' interests are typically in line with those of law enforcement and they therefore enact statutes that favor expansive police authority. Yet, when it comes to iPhones the situation might be different. Unlike the faceless backdrop in which legislators typically award police great investigatory powers, the scenarios in which an iPhone can be searched incident to arrest are likely to resonate with legislators.

As typically middle- or upper-class individuals with teenage or young adult children, legislators are one of the demographic groups likely to purchase iPhones. And while legislators rarely commit the crimes of murder or rape, as mostly middle-class white men they are statistically more likely to be involved in computer crimes such as financial misconduct or fraud. It is evidence of these crimes that is most likely to accidentally turn up during a search of an iPhone incident to an arrest, whether for running a stop sign or driving while intoxicated. Moreover, while legislators are unlikely to have illegal child pornography on their computers or iPhones, it is reasonable to assume many legislators have downloaded "run-of-the-mill" pornography. While this material is not illegal, its discovery would be embarrassing and politically devastating.

Significant legislative protections for criminal defendants often arise in response to a particular legislator being put through the criminal justice process. Thus, while legislators are tough on crime and reluctant to reduce punishments or remove old crimes from the books, it is reasonable to expect that legislators will create criminal procedure protections that track their own self-interest. It is therefore possible that legislators will enact laws limiting the search of iPhones incident to arrest.

Moreover, legislators have incentive to enact such restrictions to please constituents. While it is unlikely that a lobbyist will form to press for a law exempting iPhones from the search incident to arrest doctrine, it is entirely possible that in the near future a prominent business executive or other powerful and connected individual will be embarrassed when his iPhone is searched at a traffic stop. And when those middle- and upper-class individuals—the type who vote and, more importantly, have money to make campaign contributions—press for some legislative action, lawmakers will have little reason to refuse them. The soft-on-crime label tends not to stick when the new law benefits a considerable majority and protects the middle-class right to privacy.

Change at the margins: open application test

A more modest revision to the search incident to arrest doctrine, but one that nevertheless would eliminate the current bright-line rule, would be for courts to adopt an open application test. Under an open application approach, police would be permitted to search any open application on the iPhone incident to arrest but would not be authorized to look through applications that are closed when the arrest is made. Thus, an individual who took steps to close the iPhone application could expect the pictures contained therein to remain private. More significantly, an individual who kept her iPhone off entirely could avoid any search of its contents.

There are at least two problems with this approach: First, it would be very difficult to know if officers are telling the truth when they say an application was open. Because an iPhone can be turned on simply by tapping the touch screen and applications can be activated simply by touching an icon, it would be easy for officers to testify that an application was open at the time of arrest, even if it was in fact closed. Of course, the prospect of police lying runs throughout Fourth Amendment jurisprudence. Police could just as easily lie and say they received consent to search the trunk of a vehicle when they in fact did not, or that they smelled marijuana when in fact there was no such smell.

A second and more compelling reason to reject the open application test is that it runs afoul of one of the original justifications for the search incident to arrest doctrine: preventing the destruction of evidence. Just as police could quickly open a closed application on the iPhone, so too could a suspect. An arrestee skilled at using his iPhone might be able to turn on the device, select an application, and destroy text messages, emails, photos, or other evidence in a matter of seconds.

Given that the Supreme Court has adopted a fiction that almost any physical evidence—whether in a closed or open container—in the arrestee's grasp could potentially be destroyed (even if the arrestee is handcuffed) it would make little sense to draw a fine forbidding searches of closed applications on an electronic device that an arrestee could easily open and destroy.

Changing bright-line rule: limiting search incident to arrest doctrine to five steps of searches

Another solution would be to limit police to only a fixed number of steps when searching the contents of an iPhone incident to arrest. For instance, courts could set a bright-line rule that police can take five steps, but no more, when rummaging through an iPhone's contents. As with the open application test, this solution likely causes more problems than it would solve, but is worth exploring briefly.

The primary virtue of the search incident to arrest doctrine is that it provides bright-line rules that are easily understood and applied. Thus, police know that they can open an arrestee's wallet but cannot search the trunk of his car. The primary detriment of the search incident to arrest doctrine is that it permits the police to rummage through numerous layers of enclosed materials, even if there is no probable cause to believe contraband is buried beneath. This problem is particularly vexing with respect to the iPhone because it contains layer upon layer of data.
cussed, police conceivably could (1) turn on the phone; (2) open an internet browser; (3) type in a web-based email account such as www.hotmail.com; (4) log into the account (if the user id and password are saved); (5) open a folder of messages; (6) open a particular message; (7) read the message; (8) open the attachment to the message; and so forth.

One compromise approach would be to create a bright-line “five-level deep” rule (or some other admittedly arbitrary number) limiting the search of iPhones to a total of five steps. Under such a rule, the police could search five levels deep into an iPhone’s contents, but no further. Thus, for example, police could (1) turn on the phone; (2) open the internet browser; (3) type in a web-based email account such as www.hotmail.com; (4) log into the account (if the user id and password are saved); and (5) open a folder of messages. If the officer completes the fifth step without finding anything incriminating that could be destroyed, the officer would need to stop searching. To search further, the officer would need to procure a warrant.

The main virtue to this approach is that it puts an outer limit on how far police may search electronic data while at the same time leaving intact a relatively bright-line rule that makes clear to police exactly how far they can go. On the other hand, whether police exceeded the five steps would certainly be debated in individual cases. Judges would have to make findings of fact ranging from the simple—whether the phone was already turned on when the search incident to arrest began, thus not counting as one of the five steps—to more fuzzy inquiries. For instance, when police linked from one webpage to another, were they taking two steps, or just one? This sort of unguided fact-finding is exactly what courts have tried to avoid by advocating a bright-line search incident to arrest rule.

Perhaps more obviously troubling, selecting a certain number of searches—for instance, saying that police can search five levels deep into an iPhone, but not six—is terribly arbitrary. While courts could say the number of levels is correlated to the likelihood that the arrestee could reach that data and destroy it, selecting a level would still be beyond the institutional capacity of courts. Moreover, no comparable five-step rule exists for searches of tangible evidence found during a typical search incident to arrest. If police can exceed five steps to discover drugs in a small bag hidden inside a box lying under some papers in the glove compartment of a car, it is difficult to justify a five-step rule only for iPhones.

Distinguishing between data on device and remotely-stored data accessible from device

Finally, courts could try to draw a conceptual line between data that is “on” or “in” the iPhone and data that is simply accessible via the iPhone. This would essentially be drawing a line between the iPhone’s internet browser function and its other applications. An arrestee’s pictures in his iPhoto application, his text messages, and his incoming call history would be considered contained “in” the phone. If internet service were cut off, the owner of the phone would still be able to access these features because the data has been downloaded to the phone. By contrast, web-based email accounts or other material that an individual accesses over the internet are not typically downloaded to the phone and are instead, for lack of a better phrase, simply floating around on electronic servers in cyberspace. Because such data is not physically present on the iPhone without proactively seeking it out, courts and legislatures could draw a line forbidding such searches incident to arrest while allowing police to search applications that have data permanently on the iPhone.

One wrinkle to this approach might be if the internet browser that allows the user to access information floating in cyberspace is open when the officer searches the iPhone. For instance, what if the officer conducting the search incident to arrest discovers that the internet browser is open to a web-based email account and the selected email has incriminating information in it? Surely it would not make sense to say that the officer could search the rest of the iPhone’s applications but not the open web-based email. One solution to this problem would be to harken back to the original search incident to arrest jurisprudence that allows a full-scale search of some areas beyond the person of the arrestee if the area is in the immediate grabbing space. For instance, the search incident to arrest doctrine typically does not allow a search of the trunk of a vehicle, but if the trunk is open and the arrestee is standing near it, then such a search is permissible. In the hypothetical scenario outlined above, web-based email can be analogized to the trunk of a car. The web-based email, banking information, or MySpace page, would typically be considered to be outside the grabbing space of the suspect. However, when the webpage is open in the internet browser at the time of arrest it would be within the arrestee’s immediate grabbing space.

Thinking in terms of physical tangible space, an approach that differentiates between material downloaded onto the iPhone and material that is simply accessible via the iPhone seems to make sense. Just as officers could search the cigarette pack in Mr. Robinson’s pocket, they can also search the photos he is carrying on his iPhone. And just as the police could not search Mr. Robinson’s medical records stored in his house (rather than on his person), the police also could not search electronic data not currently downloaded onto his phone.

Yet, the comparison with Robinson’s medical records fails at a certain level when we consider that one purpose of the search incident to arrest doctrine is to prevent destruction of evidence. Of course, Mr. Robinson could not destroy the medical records in his house while being arrested at a traffic stop. Yet, he could quickly open his internet browser, log onto his web-based email account, and destroy incriminating evidence without ever leaving the traffic stop. Nevertheless, this approach is conceptually promising because it does not require a wholesale revision of the search incident to arrest doctrine, which has been framed with tangible physical evidence in mind.

Conclusion

At the end of the day, all of the approaches outlined above appear to be somewhat unsatisfying. Permitting the police to search only for evidence related to the purpose of arrest would improve the doctrine for all cases, not just those involving iPhones, but it has recently been rejected by a majority of the Supreme Court. Asking state legislatures to limit police to search incident to arrest only for evidence related to the arrest is plausible, but highly unlikely to occur in many states. An open application test may encourage police deception and will likely create the types of factual disputes that the bright-line search incident to arrest doctrine was designed to avoid. A five-step limit will likewise raise factual questions that are best avoided. Finally, while a rule that differentiates between data on the iPhone and data accessible via the phone is the most conceptually pure, it does not account for the possibility that arrestees could still destroy data that is merely accessible via the iPhone. Nevertheless, despite the flaws associated with each proposal, all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant.