William & Mary Bill of Rights Journal

Volume *Volume 22 (2013-2014)*
Issue 2 *Professor Charles H. Koch, Jr. Memorial Symposium on Administrative Law*
Article 15

December 2013

Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem

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

SEIZING A CELL PHONE INCIDENT TO ARREST: DATA EXTRACTION DEVICES, FARADAY BAGS, OR ALUMINUM FOIL AS A SOLUTION TO THE WARRANTLESS CELL PHONE SEARCH PROBLEM

Adam M. Gershowitz*

When police conduct a lawful custodial arrest, can they search the cell phone in your pocket? Numerous courts have reached conflicting conclusions on this question. This Article argues that police should only be permitted to seize cell phones incident to arrest. If the police are concerned about data being remotely wiped from the phone while they wait for a search warrant, the officers should preserve the data by using either a data extraction device to copy the phone's contents, an inexpensive bag called a Faraday cage to prevent remote wiping of the cell phone, or a simple sheet of aluminum foil to immobilize the phone.

Under the search incident to arrest doctrine, police have long been permitted to open any item on an arrestee, whether they have probable cause for that particular item or not.[1] The rationale is that arrestees could try to destroy evidence or use hidden objects to harm officers.[2] And because police conduct millions of searches per year,[3] the Supreme Court has established a bright-line rule.[4] Decades of precedent therefore seem to indicate that police can search through the full contents of any item on an arrestee, including electronics.[5]

But surely cell phones must be different. After all, while wallets hold business cards and a few scraps of paper, cell phones contain thousands of pictures, emails, Facebook information, Internet browsing history, and map locations—and that is just the information accessible from the first screen of the device. If the police can search your cell

* Professor of Law, William & Mary Law School. I am grateful to Jeff Bellin and Paul Marcus for helpful suggestions and to Jake Derr and Peter Landsman for research assistance.

[1] *See* United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that police officers may search one's person incident to arrest, including any containers on the person); Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL'Y REV. 381, 394 (2001).

[2] *See* Logan, *supra* note 1, at 391–92 (citing Chimel v. California, 395 U.S. 56 (1950)).

[3] *See, e.g.*, Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 47 (2008) [hereinafter Gershowitz, *The iPhone Meets the Fourth Amendment*].

[4] *See Robinson*, 414 U.S. at 235 (holding that the search incident to arrest doctrine is automatic, regardless of the actual presence of the doctrine's rationale).

[5] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 3, at 38–39 (discussing the lack of "any conceptual difference between searching a person's body or physical containers on that body for drugs and searching electronic equipment for digital information," as first recognized by the Fifth Circuit).

phone incident to arrest, then they can search your entire life. And they would have this power even if they arrested you for a low-level crime—think of public intoxication, petty theft, or even texting while driving[6]—because longstanding doctrine indicates that the scope of the search has no relation to the severity of the crime of arrest.[7]

In these circumstances, what are courts to do? Should they follow decades of precedent from the pre-Internet era even though that seems illogical? Or should they disregard controlling Supreme Court precedent and try to carve out a new search incident to arrest rule that would only apply to cell phone searches?

This Article suggests that the lower courts (and eventually the Supreme Court) should only allow police to seize cell phones incident to arrest. Then, while waiting for a search warrant, police should preserve the cell phone data by using either a data extraction device to copy the phone's contents, an inexpensive bag called a Faraday cage to prevent remote wiping of the cell phone, or a simple sheet of aluminum foil to immobilize the phone.

After briefly surveying the state of the law, I review some of the other proposals for limiting cell phone searches and explain why they are flawed.[8] I then explain the practical ease with which police would be able to seize a phone and preserve its data while waiting for a search warrant.[9] Finally, I review previous instances in which the Court has allowed warrantless seizures, but not searches, and demonstrate how cell phones fit squarely into that paradigm.[10]

I. THE STATE OF THE LAW: CONFUSION AND INCONSISTENCY

The initial response by most courts to warrantless cell phone searches incident to arrest was to rely on Supreme Court precedent for tangible items.[11] Led by the U.S. Court of Appeals for the Fifth Circuit,[12] most courts concluded that cell phones are containers in the same way that wallets, pockets, and purses are containers, and that the phones can therefore be searched incident to arrest.[13] By 2010, more than thirty courts

---

[6] *See* Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 ARIZ. L. REV. 577, 593–96 (2012).

[7] *See, e.g.*, *Robinson*, 414 U.S. at 236–37 (holding that an arrest for driving with a revoked license gave police officers sufficient authority to search the arrestee without additional justification).

[8] *See infra* Parts I, II.

[9] *See infra* Part III.

[10] *See infra* Part IV.

[11] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 3, at 38–40.

[12] *See* United States v. Finley, 477 F.3d 250 (5th Cir. 2007).

[13] *See* Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1137–38 n.66 (2011) [hereinafter Gershowitz, *Password Protected?*] (listing numerous recent opinions upholding the legality of warrantless cell phone searches incident to arrest).

had issued opinions approving warrantless cell phone searches incident to arrest.[14] As the years ticked on and cell phone technology became more sophisticated, however, courts began to challenge the conventional wisdom.[15] In a prominent decision, the Ohio Supreme Court prohibited warrantless cell phone searches incident to arrest because cell phones "are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container."[16] A smattering of lower courts joined suit.[17] And in May 2013, the Florida Supreme Court[18] and the U.S. Court of Appeals for the First Circuit[19] both concluded that police are not permitted to conduct a warrantless cell phone search simply because they have first arrested the phone's owner.

As of mid-2013, dozens of courts have issued rulings on the constitutionality of warrantless cell phone searches, and there is a considerable split among state supreme courts and federal circuits.[20] On one side, the majority of courts, including the California Supreme Court,[21] as well as the U.S. Courts of Appeals for the Fourth,[22] Fifth,[23] Seventh,[24] Tenth,[25] and Eleventh Circuits[26]—have approved warrantless searches. On the other side, the Ohio Supreme Court,[27] the Florida Supreme Court,[28] the First Circuit Court of Appeals,[29] and various lower state and federal courts have rejected warrantless searches.[30] It seems inevitable that the Supreme Court of the United States will grant certiorari on this issue in the near future.[31] But then what? With the technology rapidly changing and the Justices not being particularly tech savvy, will the Court be able to fashion a workable rule?

---

[14] *Id.* at 1139.

[15] As Judge Posner described in 2012, "analogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life." United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012) (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) (internal quotation marks omitted)).

[16] State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

[17] *See* Gershowitz, *Password Protected?*, *supra* note 13, at 1139 n.76.

[18] *See* Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013).

[19] *See* United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013).

[20] *See infra* notes 21–30 and accompanying text.

[21] *See* People v. Diaz, 244 P.3d 501, 505–06 (Cal. 2011).

[22] *See* United States v. Murphy, 552 F.3d 405, 410–12 (4th Cir. 2009).

[23] *See* United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007).

[24] *See* United States v. Pineda-Areola, 372 F. App'x 661, 663 (7th Cir. 2010).

[25] *See* Silvan W. v. Briggs, 309 F. App'x 216, 225 (10th Cir. 2009).

[26] *See* United States v. Fuentes, 368 F. App'x 95, 99 (11th Cir. 2010) (per curiam).

[27] *See* State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

[28] *See* Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013).

[29] *See* United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013).

[30] For other cases rejecting the search incident to arrest of cell phones, see Gershowitz, *Password Protected?*, *supra* note 13, at 1139 n.76.

[31] *See* Orin Kerr, *First Circuit Rules that Police Need a Warrant to Search a Cell Phone Incident to Arrest*, VOLOKH CONSPIRACY (May 17, 2013, 4:26 PM), http://www.volokh.com/2013/05/17/first-circuit-rules-that-police-need-a-warrant-to-search-a-cell-phone-incident-to-arrest/.

II. THE FLAWS OF PROPOSED SOLUTIONS

Scholars have weighed in with numerous suggestions, but they all suffer flaws. For instance, in an earlier article, I suggested that police be permitted only to search open applications on a phone, or that they be permitted only to take a certain number of steps to open additional applications.[32] But such a rule is arbitrary and promotes police lying.[33] Another proposal is to allow the police to search the phone incident to arrest only when there is reason to believe evidence related to the crime of arrest could be found, as the Court now does with searches of automobiles incident to arrest.[34] This would reduce the extent of warrantless searches (a good thing), but would mire courts in retrospective fact-bound questions about whether there was reason to believe evidence could be found in the phone. A third alternative would be to change nothing and have cell phones be governed by precedent designed for the tangible world.[35] But, as noted above, this would allow police to search huge amounts of private data with no particularized suspicion. A fourth possibility would be to simply ban all cell phone searches without a warrant.[36] This idea, without anything more, would be troubling because police would be powerless to prevent a suspect or co-conspirator from remotely wiping the phone while the police await a warrant.[37] None of these solutions, therefore, strikes an effective balance between protecting private information and permitting the police to capture evidence that could easily be destroyed before a warrant can be procured.

III. THE BETTER APPROACH: WARRANTLESS SEIZURES AND DATA PROTECTION

A better solution would be to fight fire with fire or, more aptly, to fight technology with technology. The Supreme Court should allow police to seize phones incident to arrest and then require the officers to procure a warrant before searching the phone. While awaiting the warrant, police should be encouraged to use existing technology

---

[32] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 3, at 53–56.

[33] *Id.*

[34] *See* Arizona v. Gant, 556 U.S. 332, 335 (2009). I first proposed this idea prior to the *Gant* decision. *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 3, at 48–49. A prominent Fourth Amendment scholar has recently endorsed this view. *See* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 406–07 (2013).

[35] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 3, at 45.

[36] *See, e.g.*, Mina Ford, Note, *The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right to Be Free from Unreasonable Searches and Seizures*, 39 FLA. ST. U. L. REV. 1077, 1102–03 (2012).

[37] As Judge Posner has observed, "remote-wiping capability is available on all major cellphone platforms; if the phone's manufacturer doesn't offer it, it can be bought from a mobile-security company." United States v. Flores-Lopez, 670 F.3d 803, 808 (7th Cir. 2012). Even without an application that remotely wipes the phone, a co-conspirator (for example, a drug-dealer's spouse) could erase data from the phone while sitting at a home computer.

that prevents the phone's data from being remotely destroyed. There are three easy options that officers could utilize: (1) a data extraction device that copies the contents on the phone onto a secure site; (2) a Faraday bag that fits around the phone and prevents data from being remotely erased; or (3) a simple piece of aluminum foil that officers can wrap around the phone and disable it. Here is how the Court should proceed.

First, the Supreme Court should forbid warrantless cell phone searches incident to arrest unless there is a specific exigency. For instance, if police arrest a key player in a drug conspiracy and have specific reason to believe that his arrest will lead to other conspirators trying to wipe incriminating text messages from a cell phone,[38] then police should be permitted to search the phone without a warrant. In such a circumstance, though, the authority to search without a warrant would come from the traditional exigency exception, not the search incident to arrest doctrine.[39] Or think of a case where a suspect is arrested in connection with a kidnapping and police want to search his cell phone for any information about the victim's whereabouts.[40] Searching without a warrant should be permitted under the exigency exception because there is a *specific* exigency, not because there is a *theoretical possibility* of destruction of evidence that could be avoided with a search incident to arrest.[41]

But would banning cell phone searches incident to arrest allow the destruction of evidence, which is the main rationale for the search incident to arrest doctrine?[42] If the Court disallowed searches of cell phones incident to arrest, would it not just be empowering criminals to remotely wipe evidence of their illegality? The answer is no because there are three simple ways that police can prevent data destruction while awaiting a search warrant.

---

[38] *See* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 n.3 (D. Or. 2012) ("One example, however, of a situation where an immediate search might be necessary is an instance where an officer had credible information that a suspect's accomplice was at a remote location and was planning to use Apple's remote-wipe program which allows an iPhone user to delete all information stored on an iPhone and restore it to factory settings with the click of a button from a remote location."). Additionally, consider an application called TigerText that "lets users remotely delete their text messages from other peoples' phones." *See* Chloe Albanesius, *Tiger Text App Lets You Remotely Delete Text Messages*, PC MAG. (Mar. 4, 2010, 4:29 PM), http://appscout.pcmag.com/mobile-apps/270582-tiger-text-app-lets-you-remotely-delete-text-messages.

[39] *See* United States v. Gomez, 807 F. Supp. 2d 1134, 1150 (S.D. Fla. 2011) (collecting cases where courts have relied on the exigency doctrine to search cell phones).

[40] *See* Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-to-Arrest Exception to the Cell Phone as "Hybrid,"* 60 DRAKE L. REV. 429, 489–90 (2012) (outlining a similar scenario involving child exploitation).

[41] *See Gomez*, 807 F. Supp. 2d at 1150–51 n.17 (noting that "while agents testified to their speculation that a cell phone could theoretically be 'wiped' remotely by an unknown third party, each agent testified that they had no reason to believe that Defendant's specific cell phone was capable of remote deletion" and rejecting the Government's exigency rationale).

[42] No one suggests that the other rationale for the search incident to arrest doctrine—police officer safety—is implicated by cell phone searches.

A. Data Extraction Devices to Copy Cell Phone Contents

The first option is for police to download and copy the data on the cell phone with a data extraction device. For instance, a company called Cellebrite manufactures the "Universal Forensic Extraction Device" (UFED), which conducts a "bit-for-bit extraction and in-depth analysis of data from thousands of mobile devices, including feature phones, smartphones, portable GPS devices, [and] tablets."[43] The U.S. Department of Justice found that the UFED could download all the photos and videos from an iPhone within ninety seconds.[44] Using a data extraction device is therefore faster and much more likely to prevent destruction of evidence than an officer manually and aimlessly searching a phone one application at a time.

When the civil liberties community learned about data extraction devices, their initial reaction was outrage. In 2011, the American Civil Liberties Union (ACLU) accused the Michigan State Police of downloading cell phone data without a warrant.[45] The Michigan State Police denied engaging in that practice, and the controversy died a quick death.[46]

With the exception of the ACLU's criticism of the Michigan State Police, there has been relatively little publicity about the UFED devices. You might therefore be surprised to learn that the devices are in use by federal law enforcement agencies, as well as police in New York, Los Angeles, Sacramento, and many smaller towns across the country.[47]

Depending on the version of the device, the UFED costs between a few thousand dollars and $11,500.[48] At that price, most police departments would be unlikely to buy multiple devices. Thus, police departments might have to look for another option to

---

[43] Petach Tikva, *Cellebrite Delivers First Physical Extraction Solution for Nokia BB5 Devices*, CELLEBRITE.COM (July 26, 2012), http://perma.cc/0rPkbrZSnMd.

[44] *See* Mike Masnick, *Michigan State Police Say It'll Cost $545k to Discover What Info It's Copying Off Mobile Phones During Traffic Stops*, TECH DIRT (Apr. 20, 2011, 10:44 AM), http://www.techdirt.com/blog/wireless/articles/20110420/01070213969/michigan-state-police-say-itll-cost-545k-to-discover-what-info-its-copying-off-mobile-phones-during-traffic-stops.shtml.

[45] ACLU of Mich., *ACLU Seeks Records About State Police Searches of Cellphones*, ACLUMICH.ORG (Apr. 13, 2011), http://www.aclumich.org/issues/privacy-and-technology/2011-04/1542.

[46] *See* Nathan Olivarez-Giles, *ACLU Concerned over Michigan State Police Extracting Data from Cellphones*, L.A. TIMES (Apr. 21, 2011, 4:50 PM), http://latimesblogs.latimes.com/technology/2011/04/aclu-concerned-over-michigan-state-police-extracting-phone-data.html.

[47] *See Huntsville Man Arrested for Child Pornography*, HUNTSVILLE ITEM (Mar. 20, 2013), http://itemonline.com/local/x2000917412/Huntsville-man-arrested-for-child-pornography (explaining that Huntsville, Texas, purchased the Cellebrite equipment with a grant); Nick Taborek, *You're Under Arrest! Hand over that iPhone*, BLOOMBERG BUSINESSWEEK (Mar. 29, 2012), http://www.business week.com/articles/2012-03-29/youre-under-arrest-hand-over-that-iphone (noting Cellebrite use by the federal government, New York, Los Angeles, and Sacramento).

[48] *See* Taborek, *supra* note 47.

briefly preserve the cell phone's data while taking the phone to the site where the UFED is located. As explained in Parts III.B and III.C below, there is an easy solution for preventing the contents of the phone from being remotely wiped.

B. Faraday Bags to Isolate the Phone and Prevent Remote Wiping

In addition to (or in lieu of) a data extraction device, police could use a fairly inexpensive option called a Faraday cage while they apply for a search warrant.[49] If you own a microwave oven, you have a Faraday cage in your home.[50] Simply put, an aluminum structure keeps radio waves from reaching the other side of the cage.[51] Companies already manufacture Faraday bags designed specifically for law enforcement to hold cell phones and prevent remote wiping.[52] Once placed into a Faraday bag, the phone can no longer communicate with the outside world and thus cannot be remotely wiped by a conspirator.[53] The U.S. Department of Justice has recommended that agents place any seized cell phone in a Faraday bag as soon as possible to avoid remote wiping.[54]

Anyone can purchase a Faraday bag for as little as thirty dollars,[55] and police departments would likely get a better price if they bought in bulk. Of course, thirty dollars' worth of equipment is burdensome if every officer in the entire police department must have a Faraday bag. But there is no need for that. Most officers will not be conducting cell phone searches. Rather, it is officers in narcotics units, those patrolling the highest crime areas where drug dealing is rampant, cops investigating child pornography, and possibly agents working on white-collar cases that would have need to quickly capture a cell phone. If officers working "regular" beats had an unusual case

[49] Judge Posner and the authors of two law review articles have considered using Faraday bags to solve the search incident to arrest problem, although neither Judge Posner nor the law review articles' authors considered the prospect of the phones being pre-programmed to delete data. *See* United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012); Charles E. MacLean, *But, Your Honor, a Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37, 50–51 (2012); Samuel J. H. Beutler, Note, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest*, 15 VAND. J. ENT. & TECH. L. 375, 395–96 (2013).

[50] *See* MacLean, *supra* note 49, at 50 n.82.

[51] *See id.*

[52] For instance, a product called "Black Hole Faraday Bag—RF Signal Isolation for Forensics, Standard Window Size" is "designed to aid law enforcement, military, and consultants in the collection, preservation, transport, and analysis of wireless evidence" and is available for sale for fifty-eight dollars on Amazon.com. *Black Hole Faraday Bag—RF Signal Isolation for Forensics, Standard Window Size*, AMAZON.COM, http://www.amazon.com/Black-Hole-Faraday-Bag-Isolation/dp/B0091WILY0 (last visited Dec. 12, 2013).

[53] *See id.*

[54] *See* U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, AWARENESS BRIEF: FIND MY IPHONE 3 (2009).

[55] *See* MacLean, *supra* note 49, at 50.

and needed to preserve cell phone data, they could call into dispatch and wait for another officer to bring a Faraday bag to the scene. There would be some chance that data could be remotely wiped during this short wait, but the chance would be very slim.[56]

The bigger problem with the Faraday bag solution is that it will not prevent the phone from erasing data that has been pre-programmed to delete after a certain period of time. There are now cell phone applications that will destroy data after a fixed period of time. The most famous example—Snapchat—allows a message to survive only for up to ten seconds,[57] but other applications such as Wickr and TigerText allow the messages to be visible for longer.[58] For instance, TigerText allows users to send a text message to another phone, but to keep the message stored on the application's servers.[59] The visual display of the message only appears on the recipient's phone for a preset period of time—anywhere from sixty seconds to five days—before the message is deleted from the phone.[60]

Applications like Wickr and TigerText pose a problem, although a very small one. Most drug dealers or child pornography users will not have their cell phone data preset for self-destruction. And while a handful might have the foresight to program the phone to delete sensitive material, Fourth Amendment rules have never turned on law enforcement's ability to capture every last piece of evidence. Rather, the Supreme Court seeks (or should be seeking) sensible bright-line rules that the police can understand and follow and which maximize privacy protection where possible. If police want a one hundred percent certainty that no evidence will be deleted from a seized cell phone while officers apply for a warrant, then police departments should invest in the Cellebrite UFED technology in order to instantly download the contents of the phone.[61]

A good analogy is the Court's 2013 decision in *Missouri v. McNeely*,[62] which rejected automatic warrantless blood draws in drunk driving cases.[63] In *McNeely*, the Government contended that when a driver refuses a breathalyzer test, the police should per se be able to draw his blood without a warrant under an exigency rationale.[64] The

---

[56] Indeed, placing a cell phone in a Faraday bag and preserving the evidence might be faster than the officer conducting an aimless search of the phone without a warrant. *See, e.g.*, Beutler, *supra* note 49, at 396. This would be particularly true if the phone were password protected.

[57] *See* Jefferson Graham, *Snapchat's Young Audience Fuels a Growth Streak*, USA TODAY (June 5, 2013, 6:26 PM), http://usatoday.com/story/tech/columnist/talkingtech/2013/06/05/snapchat-growth-streak/2359129/.

[58] *See* Lorenzo Franceschi-Bicchierai, *Wickr: Can the Snapchat for Grown-Ups Save You from Spies?*, MASHABLE (Mar. 4, 2013), http://mashable.com/2013/03/04/wickr/; Belinda Luscombe, *TigerText: An iPhone App for Cheating Spouses?*, TIME (Feb. 26, 2010), http://www.time.com/time/business/article/0,8599,1968233,00.html.

[59] *See* Luscombe, *supra* note 58.

[60] *See id.*

[61] *See* discussion *supra* Part III.A.

[62] 133 S. Ct. 1552 (2013).

[63] *Id.* at 1568.

[64] *Id.* at 1560. While the Court rejected a per se rule, it left the door open to some warrantless blood draws on a case-by-case basis. *Id.* at 1561.

Government argued that it needed warrantless blood draws because not having a prompt blood test around the time of arrest would make it more difficult to convince juries to convict defendants in drunk driving cases.[65] The Court was not moved by the argument that making life slightly harder for law enforcement in a small percentage of cases supported a warrantless search.[66] If jurisdictions want to have stronger drunk-driving prosecutions, they can spend the money to have judges on call to sign warrants in the middle of the night.[67]

It is true that using Faraday bags would be slightly more expensive than warrantless searches and carry a small risk of evidence destruction. But just as in the blood draw situation, the Court has never guaranteed the police the cheapest and easiest way to gather evidence.

C. Aluminum Foil: The Cheap and Simple Solution

A final solution is remarkably simple: aluminum foil. The primary material for making a Faraday bag is aluminum foil.[68] Anyone—including the police—can watch an instructional YouTube video about building a Faraday device.[69] Or, if the police do not want to build a structure, they can simply buy a roll of aluminum foil for two dollars in a grocery store and leave it in their vehicle. When the police seize a phone, they simply have to wrap the phone in a few layers of aluminum foil, and the chance of remote wiping of the phone will be almost completely eliminated.[70]

As with a Faraday bag, the aluminum foil method may not prevent one hundred percent of evidence from being wiped from the phone while police await a warrant, but it should come very close. Police departments that are strapped for cash could embrace the aluminum foil solution and be left in nearly the same position as if they had purchased UFEDs, used Faraday bags, or even conducted warrantless cell phone searches.

---

[65] *See id.* at 1565.

[66] *Id.* at 1565–66.

[67] For a similar example, consider the Court's recent decision holding that the use of a drug-sniffing dog on the porch of a home constitutes a Fourth Amendment search. *See* Florida v. Jardines, 133 S. Ct. 1409 (2013). In light of that decision, officers investigating drug activity at a home must obtain probable cause from another source, perhaps an airplane flyover, *see* California v. Ciraolo, 476 U.S. 207 (1986), or an informant assigned to go into the house and report back on any drugs inside, *see* United States v. White, 401 U.S. 745 (1971). These alternatives are surely more expensive and time-consuming, but that does not somehow make the drug-sniffing dog automatically reasonable. *See Jardines*, 133 S. Ct. at 1417.

[68] *See Make a Faraday Cage Wallet*, WIRED, http://howto.wired.com/wiki/Make_a_Faraday_Cage_Wallet (last modified Oct. 16, 2008, 10:56 PM).

[69] *See, e.g.*, *How to Make a Faraday Wallet*, YOUTUBE (May 12, 2011), http://www.youtube.com/watch?v=C9J28juJPuo.

[70] For a video example, see David Nash, *Aluminum Foil Faraday Cage Test*, YOUTUBE (Jan. 17, 2012), http://www.youtube.com/watch?v=nfDQBo3MM0I (using only one layer of aluminum foil). As with the more traditional Faraday bag, there is still a chance that the phone is pre-programmed to delete valuable data by itself without contact from an outside signal.

IV. PRECEDENT SUPPORTING WARRANTLESS SEIZURES WHILE AWAITING A SEARCH WARRANT

The big question is whether the Supreme Court would be on firm footing in allowing police to seize a phone incident to arrest, but requiring a warrant before permitting a search of the phone's contents. The answer would seem to be yes.

The most analogous comparison is the Court's 2001 decision in *Illinois v. McArthur*.[71] The police had probable cause to believe McArthur had marijuana in his house, but they lacked a warrant to enter.[72] Rather than entering and searching without a warrant, the officers took the less invasive action of preventing McArthur from entering his home for two hours while they applied for a warrant.[73] McArthur moved to suppress the marijuana and related contraband on the ground that the police had seized him for a lengthy period of time without a warrant.[74] The Supreme Court rejected that argument, explaining that "[w]e have found no case in which this Court has held unlawful a temporary seizure that was supported by probable cause and was designed to prevent the loss of evidence while the police diligently obtained a warrant in a reasonable period of time."[75] The Court praised the police officers for utilizing "a restraint that was both limited and tailored reasonably to secure law enforcement needs while protecting privacy interests."[76]

The Court's *Terry v. Ohio*[77] doctrine also supports the idea that sometimes the police should be permitted to seize but not search.[78] For instance, in a decision thirty years ago, the Court explained that if police have reasonable suspicion that a piece of luggage contains drugs, they can detain the suitcase, effectively seizing it without a warrant,

---

[71] 531 U.S. 326 (2001). The Court has reached similar conclusions in other cases. *See, e.g.*, Segura v. United States, 468 U.S. 796, 810 (1984) (opinion of Burger, C.J.) ("[A] seizure affects only possessory interests, not privacy interests. Therefore, the heightened protection we accord privacy interests is simply not implicated where a *seizure* of premises, not a search, is at issue. We hold, therefore, that securing a dwelling, on the basis of probable cause, to prevent the destruction or removal of evidence while a search warrant is being sought is not itself an unreasonable seizure of either the dwelling or its contents. We reaffirm at the same time, however, that, absent exigent circumstances, a warrantless search . . . is illegal."); United States v. Chadwick, 433 U.S. 1, 13 n.8 (1977) (rejecting a warrantless search of a footlocker and noting that "[a] search of the interior was therefore a far greater intrusion into Fourth Amendment values than the impoundment of the footlocker").

[72] *McArthur*, 531 U.S. at 328.

[73] *Id.* at 329.

[74] *Id.*

[75] *Id.* at 334.

[76] *Id.* at 337.

[77] 392 U.S. 1 (1968).

[78] *See generally id.* (articulating the view that reasonable suspicion gives police officers the right of protective seizure and limited search of a person—a "stop-and-frisk"—without violating the Fourth Amendment).

while awaiting a drug dog.[79] The officers would not be able to open that luggage without a warrant, however, even if they had probable cause for it.[80]

CONCLUSION: A SIMPLE RULE THAT PROTECTS PRIVACY WITHOUT LOSING EVIDENCE

In the cell phone context, there is very good reason for the Court to adopt a rule only allowing warrantless seizures. First, it is the simplest rule for police to implement. If police are only allowed to seize a cell phone incident to arrest, they do not have to determine whether it is reasonable to believe the phone will carry evidence related to the crime of arrest. Nor would they have to determine what functions on the phone they may search. Officers also would not have to guess how long they are permitted to search through the reams of photos, videos, emails, text messages, and other data that could take hours to review. In addition to simplicity, a rule that only allows a warrantless seizure of the phone is far more protective of privacy than authorizing a warrantless search of the data on the phone. No suspect wants her phone to be seized, but almost everyone would prefer that the police have to obtain permission from a neutral magistrate before officers search the phone.[81] Indeed, in some cases, the magistrate may refuse to issue the search warrant or may impose limits on what functions and applications the police can search on the phone. Finally, police can seize the phone without any serious risk of losing evidence. Many police departments are already using technology that enables them to download an exact copy of the phone's data. Police departments

---

[79] *See* United States v. Place, 462 U.S. 696, 700 (1983) (finding detention to be unreasonable in this case because police took the luggage for ninety minutes and brought it to an airport across town).

[80] In the late 1970s and 1980s, the Court also embraced a rule that authorized warrantless seizures (but not searches) of packages found in automobiles. *See* Arkansas v. Sanders, 442 U.S. 753, 766 (1979). Unfortunately, the Court made this rule too confusing (and too easy to manipulate) by also approving warrantless searches if police had probable cause for the entire vehicle, rather than just the package. *See* United States v. Ross, 456 U.S. 798, 825 (1982). By 1991, the Court gave up the effort to draw a distinction between a car that happens to turn up a container and a container that happens to turn up a car. *See* California v. Acevedo, 500 U.S. 565 (1991). Under the current rule, "police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained." *Id.* at 580.

[81] As Justice Harlan explained (unsuccessfully) in the automobile exception context, "the lesser intrusion will almost always be the simple seizure . . . [that] enable[s] the officers to obtain a search warrant." Chambers v. Maroney, 399 U.S. 42, 63 (1970) (Harlan, J., concurring in part and dissenting in part); *see also* James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417, 1469 n.283 ("There is a plausible argument that the damage done to privacy interests by the search of a vehicle (and its contents) is markedly more severe than the damage done to possessory interests by a seizure of that same vehicle, and, as a consequence, that officers should be compelled to choose the seizure alternative so that if they are wrong in their probable cause assessments the less serious injury will be inflicted.").

that lack the funds to purchase data extraction devices can utilize inexpensive Faraday bags to prevent remote wiping of the phone. And departments truly strapped for cash can equip their officers with a two-dollar roll of aluminum foil that will likewise prevent almost all data loss.

Police departments might prefer to have unrestricted authority to conduct warrantless cell phone searches incident to arrest. But the Fourth Amendment does not guarantee the police the most convenient searching method. And in a world where tremendous amounts of private data are held on cell phones, giving officers carte blanche to conduct warrantless and even suspicionless searches makes little sense when simple, cheap, and effective alternatives exist. The Supreme Court should therefore resist the urge to create a complicated rule to deal with warrantless cell phone searches. It should simply prohibit warrantless searches, allow police to seize the phones, and let evolving technology handle the rest.