The Search for a Limited Search: The First Circuit Denies the Search of Cell Phones Incident to Arrest in United States v. Wurie

Evan O'Connor
Boston College Law School, evan.oconnor@bc.edu

Follow this and additional works at: http://lawdigitalcommons.bc.edu/bclr

Part of the Communications Law Commons, Criminal Law Commons, Criminal Procedure Commons, Evidence Commons, Internet Law Commons, Law Enforcement and Corrections Commons, and the Science and Technology Law Commons

Recommended Citation

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.
THE SEARCH FOR A LIMITED SEARCH: 
THE FIRST CIRCUIT DENIES THE SEARCH 
OF CELL PHONES INCIDENT TO ARREST 
IN UNITED STATES v. WURIE

Abstract: On May 17, 2013, the U.S. Court of Appeals for the First Circuit in United States v. Wurie held that the warrantless search of a cell phone was not justified by the search-incident-to-arrest exception to the Fourth Amendment and was thus an illegal search. In doing so, the court declined to agree with other federal appeals court solutions regarding this issue; most notably, the Fifth Circuit’s 2007 decision in United States v. Finley and the Seventh Circuit’s 2012 decision in United States v. Flores-Lopez. This Comment argues that the approaches taken by courts on both sides of the issue have severe vulnerabilities. It also posits that, on review, the U.S. Supreme Court should adopt a test that limits the police search to information that can be found on the phone without accessing the internet. By drawing a line regarding the searchable information in a phone, this test provides a more effective method of balancing the various concerns this issue raises.

INTRODUCTION

Since the late 1960s, the U.S. Supreme Court has held that warrantless searches of a defendant’s person can be legal under the Fourth Amendment if the searches are performed incident to an arrest.¹ The advent of smartphones, however, has created a unique and complicated challenge to this well-established legal doctrine.² With the growth and spread of advanced cell phones, courts have been forced to tackle the question of whether the exception to the Fourth Amendment’s general prohibition of warrantless searches extends to these devices.³ Although many courts have


³ See, e.g., United States v. Flores-Lopez, 670 F.3d 803, 804 (7th Cir. 2012) (addressing this question when police searched through a phone to obtain its number); United States v. Finley, 477 F.3d 250, 254 (5th Cir. 2007) (addressing this question when police searched through an arrestee’s
agreed that the exception does extend to cell phones, courts have not come to a consensus over the justification behind such an extension.\(^4\) Furthermore, several courts have taken the opposite stance, albeit with a similar divergence in their reasoning.\(^5\)

In 2013, the U.S. Court of Appeals for the First Circuit, in *United States v. Wurie*, held that the search-incident-to-arrest exception did not authorize the warrantless search of information on a cell phone seized from an arrestee’s person.\(^6\) The court decided that the preservation of evidence concerns underlying the exception were too minimal to justify such an invasive search of a device that carries a heightened expectation of privacy.\(^7\) Like other courts that have confronted the issue, the First Circuit devised a bright-line rule that applies to any kind of search, on any cell phone.\(^8\)

Part I of this Comment introduces the development of the search-incident-to-arrest exception to the Fourth Amendment and provides the factual and procedural background to *Wurie*.\(^9\) Part II explores the differing approaches courts have taken in reaching conclusions regarding how the exception applies to cell phone searches.\(^10\) Finally, Part III discusses common vulnerabilities that appear in courts’ analyses on both sides of the issue.\(^11\) In

\(^4\) Compare Flores-Lopez, 670 F.3d at 809 (analyzing the policies underlying the search-incident-to-arrest exception—including preservation of evidence concerns—in extending the exception to the warrantless search of a cell phone), with Finley, 477 F.3d at 259–60 (rejecting the need to conduct a more in-depth examination of the search-incident-to-arrest exception’s underlying policies in extending the exception), and People v. Diaz, 244 P.3d 501, 505–06 (Cal. 2011) (relying on the categorization of cell phones as containers in extending the exception).

\(^5\) Compare United States v. Park, No. CR 05–375 SI, 2007 WL 1521573, at *9, *12 (N.D. Cal. May 23, 2007) (placing cell phones under the immediate area of control branch of search-incident-to-arrest analysis and concluding that the resulting analysis failed to justify the search), with Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013) (refusing to characterize searches of cell phones with traditional search-incident-to-arrest definitions and instead relying on the level of intrusiveness to find that the exception did not apply), and State v. Smith, 920 N.E.2d 949, 955 (Ohio 2011) (holding that the warrantless searches of cell phones are outside the scope of the search-incident-to-arrest exception because of a higher expectation of privacy accompanying the devices).


\(^7\) See id.

\(^8\) Id. (indicating that the search-incident-to-arrest exception can never justify the warrantless search of cell phones); see also Finley, 477 F.3d at 260 (concluding that the search-incident-to-arrest exception justifies all searches of cell phones when accompanied by a lawful arrest). But see Flores-Lopez, 670 F.3d at 809 (declining to extend its ruling beyond similar facts due to the reluctance to address the question of increasingly invasive phone searches).

\(^9\) See infra notes 13–38 and accompanying text.

\(^10\) See infra notes 39–64 and accompanying text.

\(^11\) See infra notes 65–94 and accompanying text.
contrast to the bright-line rules adopted by many courts—including the First Circuit in Wurie—this Comment posits that a more nuanced approach better balances the policies underlying the search-incident-to-arrest exception with Fourth Amendment concerns: the U.S. Supreme Court should permit warrantless searches of cell phones, but limit them to information that does not require Internet access.12

I. LEGAL LANDSCAPE BEHIND THE SEARCH-INCIDENT-TO-ARREST EXCEPTION AND WARRANTLESS SEARCHES OF CELL PHONES

A. Fourth Amendment and the Development of the Exception

The Fourth Amendment protects the right of American citizens to be free from unreasonable searches and seizures against their person, homes, and property.13 Consequently, warrantless searches and seizures are per se unreasonable, unless a specific exception applies.14 One such exception is the search-incident-to-arrest exception, which can be conducted after a lawful arrest has been made.15 The current search-incident-to-arrest analysis, however, is a fairly recent phenomenon and is still developing.16

The U.S. Supreme Court has clarified that the search-incident-to-arrest exception only applies to the extent necessary to further evidentiary and

---

12 See infra notes 82–94 and accompanying text.
13 U.S. CONST. amend. IV; see also Blane M. Michael, Reading the Fourth Amendment: Guidance from the Mischief that Gave it Birth, 85 N.Y.U. L. REV. 905, 907–09 (2010) (explaining that the amendment arose out of American colonial reaction to British search and seizure practice, including infamous writs of assistance, which granted easy access to warrantless searches of person and property). Although the framers of the Constitution likely did not foresee this result, the Fourth Amendment has become the foundation for regulating our entire system of law enforcement. Daniel J. Solove, Fourth Amendment Pragmatism, 51 B.C. L. REV. 1511, 1516 (2010).
15 Gant, 556 U.S. at at 339 (quoting Chimel, 395 U.S. at 763). The freedom of police officers to conduct a warrantless search of the arrestee’s person immediately after an arrest has been a pillar of the American and English criminal procedure traditions. See Weeks v. United States, 232 U.S. 383, 392 (1914) (recognizing that English and American law have uniformly maintained this right); see also Wayne A. Logan, An Exception Swallows a Rule: Police Authority to Search Incident to Arrest, 19 YALE L. & POL’Y REV. 381, 387 (2001) (describing how the exception evolved from a limited right, in line with the framers’ reluctance to grant discretionary authority to law enforcement, into today’s broader interpretation).
16 See George M. Deryl III, A Case of Doubtful Certainty: The Court Relapses into Search Incident to Arrest Confusion in Arizona v. Gant, 44 IND. L. REV. 395, 396 (2011) (highlighting new challenges that will develop in Fourth Amendment jurisprudence and positing that recent decisions have created ambiguities).
safety concerns.17 In 1969, in Chimel v. California, the Court thus limited the application of the exception to the arrestee’s person or the arrestee’s immediate area of control.18 The Court reasoned that searches of evidence found on the arrestee’s person or in their immediate area of control were justified by concerns of officer safety and the destruction of evidence.19 Accordingly, the Court later clarified that, unlike items found on the arrestee’s person, items in the arrestee’s immediate area can no longer be searched when the items come under the exclusive control of the police.20

Nevertheless, under some circumstances, searches incident to arrest can be sufficiently justified by the theoretical concerns of preservation of evidence and police officer protection, even if those concerns are not necessarily present in fact.21 In 1973, in United States v. Robinson, the U.S. Supreme Court held that a search incident to a custodial arrest was legal even without specific concerns that the arrestee posed a threat to the officers or that any evidence was at risk.22 In the custodial arrest context, therefore, justifications are presumed to be present.23 In other contexts, however, it may be necessary to show the existence of the justifications in fact, rather than merely relying on theoretical support.24

18 395 U.S. at 762–63.
19 Id. at 763.
21 United States v. Robinson, 414 U.S. 218, 235 (1973) (explaining that all custodial arrests would be treated alike for purposes of whether the justifications were present).
22 Id. at 236. In this case, the police searched a cigarette box on the arrestee’s person, which contained heroin. Id. at 223. The Court held that the police could always search closed containers found on the arrestee’s person incident to an arrest. Id. at 236.
24 See Chadwick, 433 U.S. at 14; Preston v. United States, 376 U.S. 364, 367 (1964). For example, the U.S. Supreme Court’s 1977 opinion United States v. Chadwick did not involve a custodial arrest, and so there was a need to point elsewhere for justification. See 433 U.S. at 14 (holding that a search of an arrestee’s footlocker was illegal where the locker had been in exclusive police custody for an hour and a half, removing any evidentiary or safety concerns); see also Preston, 376 U.S. at 367 (holding that, outside of a custodial arrest, if there is no possibility that an arrestee could reach into an area that officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply).
B. Factual and Procedural History of United States v. Wurie

In *Wurie*, the First Circuit confronted the issue of whether the search-incident-to-arrest exception applies to searches of cell phones.\(^{25}\) On the evening of September 5, 2007, police arrested Brima Wurie for the suspected sale of drugs.\(^{26}\) When Wurie arrived at the station, but before he was booked, the police discovered a cell phone on his person.\(^{27}\) The officers searched through the cell phone’s call log and contacts folder to determine Wurie’s home phone number.\(^{28}\) Using that number, the officers determined Wurie’s address, which they then searched, finding contraband.\(^{29}\)

Wurie was charged with possession with intent to distribute, distributing cocaine base, and being a felon in possession of a firearm and ammunition.\(^{30}\) Wurie filed a motion to suppress the evidence obtained as a result of the warrantless search of his cell phone.\(^{31}\) The U.S. District Court for the District of Massachusetts denied Wurie’s motion to suppress, concluding that the search of the phone number associated with the “my house” contact was no different than the search of other personal containers found on the defendant’s person.\(^{32}\) Thus, the court found that the search fell within the search-incident-to-arrest exception.\(^{33}\) A jury ultimately found Wurie guilty of all three counts and he was sentenced to 262 months in prison.\(^{34}\)

On appeal, a divided panel of the First Circuit reversed the denial of the motion to suppress, vacated Wurie’s conviction, and remanded the case for further proceedings.\(^{35}\) The court held that the search-incident-to-arrest exception did not authorize the warrantless search of data on a seized cell phone because Wurie was not a threat to an officer and there was not an

---

\(^{25}\) 728 F.3d at 1.


\(^{27}\) *Id.* at 107.

\(^{28}\) *Id.* The police had noticed that Mr. Wurie’s phone was repeatedly receiving calls from a number classified as “my house.” *Id.* The officer searched through the phone’s call log and contacts folder to determine the number associated with that contact. *Id.*

\(^{29}\) *Id.*

\(^{30}\) *Id.* at 105.

\(^{31}\) *Id.* During the search of Mr. Wurie’s apartment, the police seized 215 grams of crack cocaine, an illegal firearm, ammunition, and drug paraphernalia. *Id.*

\(^{32}\) *Id.* at 110.

\(^{33}\) *Id.*

\(^{34}\) *Wurie*, 728 F.3d at 2.

interest in preserving evidence on his cell phone. In particular, the court described the alternative ways in which police officers could preserve the evidence of an arrestee’s cell phone. For example, an officer could turn off the phone, place it in a protective enclosure, or copy the memory without looking at it.

II. THE VARYING APPROACHES TAKEN BY COURTS ON BOTH SIDES OF THE ISSUE

Thus far, courts facing the issue of cell phone searches incident to arrest have split regarding whether or not they should be allowed. Regardless of the ultimate conclusion, courts on both sides of the issue have adopted different approaches behind their decisions. Section A outlines the various approaches taken by courts that have upheld the warrantless searches of cell phones as valid searches incident to arrest. Section B then explores the various approaches taken by courts that have refused to extend the search-incident-to-arrest exception to warrantless cell phone searches.

A. The Different Reasoning Behind Courts’ Decisions to Allow Warrantless Searches of Cell Phone Data

Many courts have allowed warrantless searches of cell phone data after a lawful arrest, but have nevertheless taken different routes in reaching that decision. Some courts apply a strict search-incident-to-arrest analysis.

36 Wurie, 728 F.3d at 12. The court reviewed the district court’s legal conclusion regarding the search of the cell phone de novo. Id. at 2 (citing United States v. Kearney, 672 F.3d 81, 88–89 (1st Cir. 2012) (reviewing a lower court’s legal conclusion about a warrantless cell phone search de novo, while noting that factual findings would be reviewed only for clear error)).

37 Id. at 11.

38 Id.

39 See infra notes 43–64 and accompanying text.

40 See infra notes 43–64 and accompanying text.

41 See infra notes 43–50 and accompanying text.

42 See infra notes 51–64 and accompanying text.

43 Compare, e.g., United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) (holding that warrantless searches of cell phones are permissible after weighing the risks of the evidence against the invasiveness), with United States v. Young, 278 F. App’x 242, 245 (4th Cir. 2008) (holding that evidentiary concerns that generally face cell phones always justify searches), and Commonwealth v. Phifer, 979 N.E.2d 210, 216 (Mass. 2012) (upholding a search of a cell phone due to the high probability of evidence and potential threats to that evidence). See generally Sara M. Corradi, Be Reasonable! Limit Warrantless Smart Phone Searches to Gant’s Justification for Searches Incident to Arrest, 63 CASE W. RES. L. REV. 943, 948–51 (2013) (describing recent cases regarding warrantless searches of smartphones).

44 United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (holding that all searches of cell phones are always automatically justified by the search-incident-to-arrest exception); see United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009) (refusing to consider the invasiveness of the
Under this approach, a search is justified if it occurred pursuant to a lawful arrest. For example, the U.S. Court of Appeals for the Fifth Circuit, in *United States v. Finley* in 2007, upheld a warrantless search of an arrestee’s cell phone where police found several messages pertaining to the arrestee’s narcotics-trafficking. The court held that as long as the search followed a valid arrest, no further justification was needed.

Alternatively, some courts have preferred a balancing test when upholding searches of cell phones. Most notably, in its 2012 decision of *United States v. Flores-Lopez*, the U.S. Court of Appeals for the Seventh Circuit weighed threats towards the evidence and officer safety against the arrestee’s countervailing interest in avoiding an invasive search. Reasoning that a search for the phone’s number was only minimally invasive, the court found that the evidentiary concerns outweighed any infringement on privacy.
B. The Different Reasoning Behind Courts Refusing to Extend the Exception to Cell Phones

Despite a majority of courts permitting the warrantless searches of cell phones, a small number of courts have not extended the search-incident-to-arrest exception to cell phone searches. As with the majority, these courts have applied different reasoning to reach this conclusion.

One court limited the reach of the exception based on the type of information generally stored on cell phones. In 2007, in United States v. Park, the U.S. District Court for the Northern District of California reasoned that the type of information stored on a phone is different from the information stored on other items that could be held on one’s person, such as a wallet or an address book. Due to the type of information stored on a phone, the court explained that cell phones could not be considered as being held on the person for purposes of a warrantless search. Instead, the court characterized a phone as an item in the arrestee’s immediate area. Accord-
ingly, the court held that the exception did not apply because the phone was in the exclusive control of the police at the time. Although stopping short of excluding all warrantless phone searches, the court set a foundation upon which future courts could expand.

A second approach declines to extend the exception because of the perception that there is a high expectation of privacy associated with the modern cell phone. According to courts that follow this approach, this higher expectation of privacy is a function of modern cell phones’ features and the quality and quantity of information stored on them.

Finally, a hybrid approach weighs the heightened expectation of privacy against the possible threats toward the evidence stored on a cell phone to conclude that the exception does not apply. Under this approach, courts—including the First Circuit in Wurie—reason that the information stored on a cell phone is often personal information that, without the phone, is otherwise off-limits during a search incident to arrest. Moreover, weighing this heightened expectation of privacy against the typical interests that justify the exception, these courts conclude that the potential threats against evi-

restee’s immediate area, the court made it significantly easier to invalidate the search. See id.; Park, 2007 WL 1521573, at *9.

See Park, 2007 WL 1521573, at *4 (reasoning that the phone was in exclusive police control because it was not searched until after the defendant was booked). It has been argued that the timing differences between Finley and Park—where the Finley search occurred immediately and the Park search occurred an hour and a half after the arrest—enabled the Park court’s different conclusion and limited the decision’s usefulness as a victory for privacy rights advocates. See Ashley B. Snyder, The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?, 46 WAKE FOREST L. REV. 155, 170 (2011) (describing the Park analysis as a forerunner for other decisions, but expressing doubt as to its standing as precedent for the proposition that warrantless phone searches cannot be justified by the search-incident-to-arrest exception).

See Park, 2007 WL 1521573, at *8; see also id. (describing the line between cell phones and computers as “increasingly blurry”).

United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008), aff’d, 343 F. App’x 564 (11th Cir. 2009); Smith, 920 N.E.2d at 955.

See Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012); Smith, 920 N.E.2d at 955. See generally Wurie, 728 F.3d at 8 (discussing the features of a cell phone that create serious privacy concerns, including information of a highly personal nature, such as photographs, text messages, audio recordings, web search and browser history, bank account records, medical records, as well as direct access to the home, via a linked camera). In the 2011 case State v. Smith, the Ohio Supreme Court refused to distinguish between smartphones and more conventional phones because it concluded that even standard phones were advancing to have features and capabilities that create the same privacy concerns. Smith, 920 N.E.2d at 954.

See Wurie, 728 F.3d at 12; Smallwood, 113 So. 3d at 738.

Wurie, 728 F.3d at 8–9 (listing the personal information stored on a cell phone, including photographs, text messages, audio recordings, browsing history, calendar appointments, web search history, purchases, financial information, and medical history); Smallwood, 113 So. 3d at 738 (comparing searches of cell phones to searches of home offices with access to cabinet drawers and desks).
vidence are minimal and can be easily mitigated. Thus, after weighing the respective interests, courts applying the hybrid approach hold that warrantless cell phone searches cannot be justified by the search-incident-to-arrest exception.

III. THE COMMON FLAWS IN THE REASONING OF BOTH SIDES AND AN OVERLOOKED ALTERNATIVE: THE INTERNET TEST

A. The Flaws in the Reasoning of Both Sides

All of the approaches that courts utilize to analyze whether the search incident-to-arrest-exception applies to cell phones suffer from serious flaws in their reasoning. The strict incident-to-arrest analysis, which automatically applies the exception to cell phone searches incident to an arrest, fails to take into account the original justifications for the search-incident-to-arrest exception. Attempting to justify an automatic application to cell phones by classifying them as containers is also problematic, as it relies too heavily on a narrow categorization of cell phones. In fact, the case law has

63 Wurie, 728 F.3d at 11 (explaining that any fears about remote wiping of the phone’s information could be mitigated by shutting off the phone, copying the phone’s contents, or placing the phone in a protective enclosure); Smallwood, 13 So. 3d at 740 (determining that the police could not have access to “the most private and personal details of an arrestee’s life” through cell phone searches simply because the phone can be carried in “a person’s pocket” and explaining that there was no actual danger of the phone’s information being remotely wiped).

64 Wurie, 728 F.3d at 12; Smallwood, 13 So. 3d at 740.


66 Compare Chimel v. California, 395 U.S. 752, 763 (1969) (indicating that the justifications behind the search-incident-to-arrest exception are the preservation of evidence and officer safety), with United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (applying the strict approach and holding that all searches of cell phones are always automatically justified by the search-incident-to-arrest exception), United States v. Young, 278 F. App’x 242, 245 (4th Cir. 2008) (same), and United States v. Wurie, 728 F.3d 1, 11–12 (1st Cir. 2013), cert. granted, 82 U.S.L.W. 3104 (U.S. Jan. 17, 2014) (No. 13-212) (applying the hybrid approach and analyzing whether evidentiary concerns were present to justify searches-incident-to-arrest of a cell phone).

67 See Arizona v. Gant, 556 U.S. 332, 345 (2009) (discussing the problems with relying heavily on a container classification). Compare Finley, 477 F.3d at 260 (justifying the automatic appli-
never made it clear that such a classification is sufficient to warrant a search incident to arrest.68

Moreover, the decisions rejecting warrantless cell phone searches also suffer from critical weaknesses.69 Take, for example, the approach that focuses on the type of information stored on cell phones to classify a phone as an object in the immediate area, as opposed to on the arrestee’s person.70 This method refuses to recognize the reality of what a cell phone is and how it is generally carried.71 Cell phones are small items that are usually carried on the person, either in pockets or handbags, rather than kept in the immediate area.72 Additionally, the approach that invalidates searches because of the high expectation of privacy is flawed because it lumps all of the information stored on a cell phone together.73 This approach fails to recognize that there are different expectations of privacy for different functions of the phone.74
The balancing approach, which weighs the arrestee’s privacy interests against evidentiary threats, suffers from the very same flaw: it treats the privacy interests of all cell phone searches the same, regardless of whether the court interprets the test in favor of or against the warrantless search of cell phones.\textsuperscript{75} Because searches of cell phones vary in terms of invasiveness, a one-size-fits-all balancing test is inadequate.\textsuperscript{76} For example, searching through a phone’s contact list is far less invasive than searching through medical or financial records on a phone.\textsuperscript{77}

These considerations demand a more nuanced test to determine the applicability of the search-incident-to-arrest exception to cell phone searches.\textsuperscript{78} Although courts on both sides have expressed that a bright-line test provides clarity to police officers with regard to their duties and limitations in the field, a bright-line test need not be all-or-nothing.\textsuperscript{79} A middle-ground solution can achieve clarity while respecting the privacy concerns of the

---

\textsuperscript{75} See Orso, supra note 65 at 187 (explaining that varying degrees of privacy expectations attach to different types of cell phone information, which may lead to different Fourth Amendment conclusions about the legality of a search); Beutler, supra note 65, at 401 (explaining that information associated with traditional versus nontraditional cell phone functions have differing privacy expectations); cf. Wurie, 728 F.3d at 8–9 (mentioning many characteristics of advanced phones, such as access to bank records, medical records, and home cameras—without discussing the availability of these applications on more basic phones).

\textsuperscript{76} See Gershowitz, supra note 65, at 45–49; Orso, supra note 65, at 187; Beutler, supra note 65, at 401.

\textsuperscript{77} See Beutler, supra note 65, at 401 (“[A]n appropriate test for the scope of a cell phone search incident to arrest should concern the function of a cell phone.”); see also Orso, supra note 65, at 187 (explaining that information such as text messages and photographs are far more private than lists of recently dialed phone numbers or address books).

\textsuperscript{78} See supra notes 65–77 and accompanying text (discussing the bright-line approaches taken by courts and rejecting each approach as flawed).

\textsuperscript{79} See Wurie, 728 F.3d at 21 (Howard, J., dissenting) (explaining that a possible solution to cell phone searches can be more moderate than an all-or-nothing approach); Beutler, supra note 65, at 396 (highlighting some of the creative possibilities that have been overlooked in favor of these all-or-nothing approaches); supra notes 82–94 (discussing a more nuanced approach). But see Wurie, 728 F.3d at 6, 12–13 (majority opinion) (highlighting that a bright-line test provides clarity); United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) (same). The courts’ fear of a more nuanced position stems from the concern that it would be too difficult for police to implement in the field. See Wurie, 728 F.3d at 6, 12–13 (expressing distaste for highly subjective and fact-specific rules because of their inherent difficulty for officers to apply); Beutler, supra note 65, at 401 (explaining that the best rule for searches of cell phones incident to arrest requires simplicity for police in the field).
arrestee. Moreover, a middle-ground solution avoids the flaws common to both extremes.

B. The Internet Test

Drawing the line at information that is available without accessing the Internet creates an easy rule while safeguarding the privacy concerns of the arrestee. Under this approach, the phone’s contact list, photos, call log, and text messages would be searchable by the police, whereas e-mail, browsing history, and most mobile applications would not.

The Supreme Court should adopt this bright-line rule, which addresses both the privacy and evidentiary concerns raised by cell phone searches. The test is not difficult for police to implement. Police can easily determine when an application requires online functionality by disabling the phone’s Internet access. Moreover, this test protects the arrestee’s privacy concerns. It leaves accessible the kind of information that the search-incident-to-arrest exception has traditionally left available to police, but

---

80 See Wurie, 728 F.3d at 21 (Howard, J., dissenting).
81 See Gershowitz, supra note 65, at 45–49 (outlining the flaws of an all-or-nothing methodology); infra notes 91–94 and accompanying text (illustrating how a middle-ground approach avoids these flaws).
82 See Wurie, 728 F.3d at 12 (explaining the need for an appropriate Fourth Amendment rule to be clear as well as consistent with constitutional rights); see also Beutler, supra note 65, at 401 (proposing a broader test that distinguishes between computer-like and traditional cell phone functions); infra notes 83–90 and accompanying text.
83 Gershowitz, supra note 65, at 56 (distinguishing between information on a cell phone and information in a cell phone); see also Beutler, supra note 65, at 400–01 (comparing these advanced phone functions to computer capabilities and arguing for their increased privacy expectations); id. at 401–02 (concluding that text messages are similar enough to pager messages that they should be similarly searchable).
85 Compare Beutler, supra note 65, at 399 (calling rules unworkable when they call for difficult tasks for police in categorizing cell phones in legal categories prior to a search), with Jim Martin, How to Turn Off 3G and Mobile Data on an iPhone, TECHADVISOR (May 16, 2013), http://www.pcadvisor.co.uk/how-to/mobile-phone/3276632/how-turn-off-3g-data-on-iphone/, archived at http://perma.cc/R8LE-KK9H (illustrating that disabling a phone’s Internet access reveals which applications require online functionality). See generally Wurie, 728 F.3d at 12 (concluding that a bright-line rule regarding cell phone searches is necessary to avoid fact-specific and subjective rules that would be difficult for officers in the field to apply).
86 See Martin, supra note 85; see also Disable the Internet Connection on Your Smartphone, KIOSKEA.NET (Jan. 2013), http://en.kioskea.net/faq/7399-disable-the-internet-connection-on-your-smartphone, archived at http://perma.cc/E4Y4-MHGK (providing instructions on how to disable cell phone internet access).
87 See Snyder, supra note 57, at 162, 164 (illustrating that the kinds of information protected by this Comment’s approach, e.g., information that can be accessed only through the Internet, yield greater privacy concerns for arrestees).
protects thousands of pages of electronic data that would otherwise be outside its reach. Finally, this test does not suffer from serious evidentiary concerns. For example, information requiring Internet access—such as the type of information that would be protected from a search-incident-to-arrest under this approach—is typically not downloaded onto the phone and would thus survive a remote wiping.

Moreover, the Supreme Court should adopt the Internet test because it overcomes many drawbacks that are present in other approaches. The test treats cell phones in a way that is consistent with how people use them in reality, rather than grouping them into poorly fitting legal categorizations or legal fictions. Furthermore, it takes into account the different types of in-

---

88 See Beutler, supra note 65, at 401 (explaining that basic information on cell phones, such as address books and call lists, are similar to items that have traditionally been subject to searches incident to arrest, whereas more advanced functions, such as e-mail and Internet access, are accompanied by higher expectations of privacy in other settings). The features that fall outside of the Internet’s scope either involve minimal privacy concerns or are similar to the other types of information that courts have allowed, such as address books, contacts, call logs, and phone numbers. Id.; see Smith v. Maryland, 422 U.S. 735, 745 (1979) (holding that there is no expectation of privacy in phone numbers dialed); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (“The expectation of privacy in an electronic repository for personal data is . . . analogous to that in a personal address book or other repository for such information.”). The features protected against a search under this approach are those that have been traditionally protected by courts both recently and in the past. See United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013), cert. denied, 82 U.S.L.W. 3095 (U.S. Jan. 13, 2014) (No. 13-186) (explaining that private materials maintain their expectation of privacy even though in digital form); United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (holding that there is an expectation of privacy in the contents of an e-mail).

89 See Gershowitz, supra note 65, at 56 (explaining that the web-based information on a cell phone is not strictly located on the phone, but instead “float[s] around on electronic servers in cyberspace”). See generally Flores-Lopez, 670 F.3d at 808 (describing the evidentiary threats to information stored on cell phones, such as remote wiping).

90 See Gershowitz, supra note 65, at 56. See generally Lendino, supra note 49 (listing the various methods for disabling smartphones remotely).

91 See Gershowitz, supra note 65, at 45–49 (highlighting problems that arise from the courts’ various all-or-nothing solutions); infra notes 92–94 and accompanying text; see also Wurie, 2013 WL4402108, at *1.

92 Compare Robinson, 414 U.S. passim (crafting a modern analysis of the search-incident-to-arrest doctrine without mentioning the necessity or sufficiency of classifying a searched item as a container), and Smith, 920 N.E.2d at 954 (concluding that the traditional definition of container includes only objects that are capable of holding other objects), with Finley, 477 F.3d at 260 (categorizing cell phones as containers to help justify the automatic application of the search-incident-to-arrest exception). Compare Yanqing Cui et al., supra note 71, at 483, 491 (illustrating that most men and women carry their cell phones on their person, whether in trousers or bags), with Park, 2007 WL 1521573, at *12 (classifying cell phones as “in the arrestee’s immediate area” rather than “on their person” to take advantage of the different analysis that comes with the distinction). See generally Jana L. Knott, Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones, 35 OKLA. CITY L. REV. 445, 480 (2010) (concluding that rationalizing searches based on legal fictions is unacceptable); Snyder, supra note 57,
formation on a phone and the different levels of privacy associated with the information. Finally, this test is applicable to all cell phone types, as it addresses the particular functions of each phone, rather than the type of phone.

CONCLUSION

The First Circuit’s decision in *United States v. Wurie* is the latest chapter in a long debate amongst courts about whether the search-incident-to-arrest exception should be extended to cover the warrantless searches of cell phones. Thus far, courts have split between two extremes, albeit grounding their decisions in varying rationales. Each of these approaches has serious flaws that weaken its constitutionality or usefulness in the field. Despite the courts’ failure to recognize them, nuanced solutions are both permissible and more effective. The U.S. Supreme Court should thus reject both extremes and adopt a bright-line Internet test that limits warrantless cell phone searches to only what can be accessed without the Internet. This test would effectively allow the police to view only information that is traditionally searchable incident to arrest, while preventing them from searching extremely private information. Importantly, this test is easy for police to follow in the field and assuages the privacy concerns of arrestees.

Evan O’Connor


at 183 (concluding that cell phone technology has evolved to the point that courts should not maintain legal fictions and categorize phones alongside address books and pagers).

93 See Gershowitz, *supra* note 65, at 57 (arguing that information stored on the phone is akin to address books and other searchable items, whereas information acquired via the Internet is much more private, such as medical records); Orso, *supra* note 65, at 187 (highlighting the different expectations of privacy between different types of information on a phone); Beutler, *supra* note 65, at 401 (describing that an appropriate rule should take the different functions of a cell phone into account).

94 See Orso, *supra* note 69, at 223 (describing conventional phones as still requiring workable standards because of their capability of storing large amounts of personal data); Beutler, *supra* note 65, at 401 (concluding that keeping the same rule for conventional phones and smartphones makes it simpler for police).