No. 13-212

In The
Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

BRIMA WURIE,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The First Circuit

BRIEF FOR RESPONDENT

JUDITH H. MIZNER
Counsel of Record
FEDERAL DEFENDER OFFICE
51 Sleeper Street, 5th Floor
Boston, MA 02210
(617) 223-8061
Judith_Mizner@fd.org

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTION PRESENTED

Does the Fourth Amendment permit a warrantless search incident to arrest of the contents of a cell phone seized from a person who has been lawfully arrested?

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

Page

STATEMENT OF THE CASE

The police seized Brima Wurie's cell phone after arresting him without a warrant for a street crack cocaine sale. *United States v. Wurie*, 728 F.3d 1, 1-2 (1st Cir. 2013). The phone, a gray Verizon LG, model that opened "almost like a book," had both an exterior and interior screen. When it began ringing in the police station during the booking process and displaying the words "my house" on the exterior caller ID screen, the police decided to search the interior of the phone, looking for a phone number and location to attach to "my house." *Id*. at 2; J.A.49. An officer opened the phone and saw a picture of a woman and child as the interior screen's "wallpaper." He pushed a button to open the call log, which showed incoming calls from "my house." He pushed another button to find the phone number associated with "my house." *Id*.

Officers used a reverse telephone directory to obtain the address associated with the "my house" number. They went to that address and found a woman and child who looked like the people in the cell phone wallpaper photo. After obtaining a warrant, they searched the house. *Id*. The cocaine, marijuana, firearm, and ammunition they found formed the basis for a drug charge and a weapons charge (counts one and three), joined with a charge arising from the street sale (count two).

The United States District Court for the District of Massachusetts denied Mr. Wurie's motion to suppress the evidence obtained from the warrantless

search of his cell phone, holding that the officers conducted a constitutionally permissible search incident to arrest. *United States v. Wurie*, 612 F. Supp. 2d 104 (D. Mass. 2009). A jury convicted Mr. Wurie after a trial and the court sentenced him to a 262-month term of imprisonment.

On appeal, the government argued that a cell phone was like any other item carried on the person and could, based simply on the fact of lawful arrest, be thoroughly searched, whether at the scene of the arrest or at the police station. *Wurie*, 728 F.3d at 6-7. The government admitted that its interpretation of the search-incident-to-arrest exception "would give law enforcement broad latitude to search any electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device such as an iPad." *Id*. at 7. The United States Court of Appeals for the First Circuit rejected this interpretation.

The First Circuit recognized that cell phones and other personal electronic devices are not like a purse, a wallet, an address book, or any other container a person may carry. The personal electronic devices used by 85% of Americans may contain vast quantities of information "of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." 728 F.3d at 8. "It is the kind of information one would previously have stored in one's home and that would have been

off-limits to officers performing a search incident to arrest." *Id*. The court also noted that additional privacy implications arose from the fact that such devices "'increasingly store personal user data in the cloud instead of on the device itself,'" and questioned the government's ability to avoid accessing such information while searching a device. *Id*. n.8.

The First Circuit reviewed this Court's search-incident-to-arrest jurisprudence from *Chimel v. California*, 395 U.S. 752 (1969), through *United States v. Robinson*, 414 U.S. 218 (1973), and *United States v. Edwards*, 415 U.S. 800 (1974), to *Arizona v. Gant*, 556 U.S. 332 (2009). 728 F.3d at 3-5. The court determined that "what distinguishes a warrantless search of the data within a modern cell phone from the inspection of an arrestee's cigarette pack or the examination of his clothing is not just the nature of the item searched but the nature and scope of the *search itself*." *Id*. at 9 (emphasis in original).

The First Circuit concluded that the warrantless search of data within a cell phone was not justified by the purposes of the search-incident-to-arrest exception, *i.e.*, officer safety and the preservation of evidence that an arrestee could conceal or destroy. 728 F.3d at 9-13. A data search was not necessary for officer safety. Nor, given available technologies, was it necessary to prevent the destruction of evidence. *Id*. at 10-11. The court explained that it was not suggesting a rule that would require a case-by-case assessment of whether a data search of a personal electronic device incident to arrest was justified by

officer safety or evidence preservation. Rather, because such searches had not been shown to ever be necessary for those purposes, it found them to be categorically unlawful. *Id*. at 12. This bright-line rule would be easy to administer in the field. *Id*. at 13. The court, however, did not forbid all on-the-spot searches of cell phones. Instead, it recognized that the exigent circumstances exception, which does require a case-specific review, would presumably allow an immediate, warrantless search of device data if there was probable cause to believe the device contained evidence of a crime and a compelling need made obtaining a warrant impracticable. *Id*. at 13.

SUMMARY OF ARGUMENT

A person today can carry a breadth and depth of private, personal information in her cell phone previously found only in the home. The seize-and-secure rule fashioned by the First Circuit permits police to seize a cell phone or other personal electronic device incident to arrest and retain control of it until a neutral magistrate determines whether it may be searched. The rule respects both law enforcement interests in obtaining evidence of crime, and the individual's interests in her papers and effects protected by the Fourth Amendment. It is a practical, easily administered rule and should be affirmed.

In *Chimel v. California*, 395 U.S. 752 (1969), the Court resolved inconsistencies in its prior definitions

of the constitutionally permissible scope of a search incident to arrest, an exception to the Fourth Amendment's warrant requirement. It explained that this exception is predicated on protecting officer safety and preventing the destruction of evidence, justifications that apply to both searches of a person placed under arrest and items seized from her person, and to searches of the area into which an arrested person can reach. The Court has repeatedly reaffirmed these principles.

While holding, in *United States v. Robinson*, 414 U.S. 218 (1973), that the police need not determine on a case-by-case basis whether these justifications were present before searching an individual's person, the Court did not hold these justifications were irrelevant or inapplicable to such searches. It did not create a special exception to the search-incident-to-arrest doctrine that wholly untethered searches of a person incident to arrest from these historical justifications. Accordingly, a search of a cell phone seized from a person that, categorically, cannot be justified as based on officer safety or the prevention of the destruction of evidence is not a constitutionally permissible search incident to arrest. For these reasons, the government's reliance on *Robinson* to justify the sweeping rule it seeks is misplaced.

No support for a warrantless search of a cell phone can be found in the limited expansion of the scope of a constitutionally permissible search of a recently vacated automobile incident to the arrest of its recent occupant established in *Arizona v. Gant*,

556 U.S. 332 (2009). *Gant* authorized a search when it is "reasonable to believe that evidence of the offense of arrest might be found," based on the "circumstances unique to the automobile context." *Id*. at 335. It should remain so limited. Automobiles have a history of different treatment under the Fourth Amendment based on their mobility and a multi-faceted reduction in reasonable expectations of privacy associated with them. Cell phones share none of the attributes of an automobile found to support the limited expansion in *Gant*.

Further, contrary to the government's claims, neither considerations of officer safety nor prevention of the destruction of evidence support the warrantless search of a cell phone incident to arrest. The contents of a phone seized by an officer cannot be used as a weapon. Its search cannot reasonably be viewed as addressing any likely threat to officer safety from others. Moreover, forensic tools and other devices can be used to prevent the destruction of evidence suspected to be contained in a phone. The contents of a phone can be copied and held, unexamined and undestroyed, until a neutral magistrate determines that there is probable cause for a particular search.

Nor does a limited warrantless search of portions of a cell phone's contents, such as its call log, fall within the scope of a constitutionally permissible search incident to arrest. Unlike the list of numbers dialed provided by a pen register or call records available from a telephone company, a cell phone's call log may often have associational data created by

the user. Moreover, a limited search rule is not readily administered in the field. An officer cannot be expected to know how to properly limit a search to only the call logs on each of the hundreds of models of cell phones available today.

In contrast to the government's limited search proposal, a seize-and-secure rule is a categorical rule requiring no item-by-item assessment of the capacities or capabilities of a particular phone by the officer in the field. The officer knows he may seize a cell phone possessed by an arrestee and hold it pending the issuance of a warrant. If deemed necessary, he may preserve the contents of the phone, unexamined. Nor does the rule preclude the application of some other exception to the warrant requirement. This Court should affirm the seize-and-secure rule as a proper balance between the law enforcement interest in investigating crime and the individual's interest in freedom from unreasonable searches and seizures.

ARGUMENT

THE FOURTH AMENDMENT DID NOT AUTHORIZE THE WARRANTLESS SEARCH OF BRIMA WURIE'S CELL PHONE INCIDENT TO HIS ARREST

As of January, 2014, ninety percent (90%) of adults in the United States owned cell phones; forty-two

percent (42%) owned a tablet computer.[1] These devices allow people to carry in their pocket or purse a breadth and depth of personal, private information previously found only in the home. "Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once." *State v. Granville*, ___ S.W.3d ___, 2014 WL 714730, at *6 (Tex. Crim. App. Feb. 26, 2014). Even the simplest cell phone is capable of storing associational information, innermost private thoughts, memos, texts, voicemails, calendars and schedules, as well as phone numbers and addresses. Current models of devices can store and/or access medical information, financial information, travels, e-mails, innumerable other documents, and one's entire library. *Smallwood v. State*, 113 So. 3d 724, 732 (Fla. 2013); *United States v. Flores-Lopez*, 670 F.3d 803, 806 (7th Cir. 2012); *State v. Smith*, 920 N.E.2d 949, 954 (Ohio 2009). All of this personal, private information may be found through searching a device. The government asks this Court to transform the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement into a blanket rule that would allow police *carte blanche* access to this information as a matter of right – an interpretation that is virtually limitless and makes no distinction between a weapon,

[1] Pew Research Center, *available at* http://www.pewresearch.org/data-trend/mobile/device-ownership/

a bag, a cigarette pack, a cell phone, a tablet, a laptop computer, or any other item a person may carry.

The FBI reports an estimated 12,196,959 arrests nationwide in 2012. This does not include data on citations for traffic violations.[2] Under the government's all-encompassing view, everyone arrested with a cell phone or tablet computer is automatically subject to a search of any and all aspects of their lives contained in that personal electronic device – regardless of the purpose of the arrest and without any connection between the device and the activity leading to the arrest. The Fourth Amendment does not authorize such an unprecedented ability to pry into the most private matters of any person arrested for any violation of law. This Court should reject the government's efforts to reformulate the scope of the search-incident-to-arrest exception by affirming the seize-and-secure rule of the First Circuit.

A. Mr. Wurie Had a Reasonable Expectation of Privacy in the Information Contained in His Cell Phone

"The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State . . . '(t)he security of one's privacy against arbitrary intrusion

---

[2] Federal Bureau of Investigation, *available at* http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/persons-arrested/persons arrested

by the police' [is] 'at the core of the Fourth Amendment' and 'basic to a free society.'" *Schmerber v. California*, 384 U.S. 757, 767 (1966). "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967) (internal citations omitted). *See also Bond v. United States*, 529 U.S. 334 (2000) (law enforcement officer's physical manipulation of bus passenger's carry-on bag violated Fourth Amendment even though bag was exposed to public). Although cell phones are frequently used in areas accessible to the public, persons have a reasonable expectation of privacy in the information contained within them.

Cell phones, like computers and tablets, are both "effects" and "papers" protected by the Fourth Amendment. These personal electronic devices may now contain or access virtually all of the "papers" traditionally kept in desks, file cabinets and boxes in the home and are among a person's most private "effects." *See*, *e.g.*, *Wurie*, 728 F.3d at 8-9. Though these devices employ technology beyond what could be imagined at the time of the framing of the Constitution, whether they may be searched without a warrant incident to arrest requires applying established Fourth Amendment principles designed to protect the integrity of individual privacy even as technology evolves over time. *See United States v. Chadwick*, 433

U.S. 1, 9 (1977) ("[T]he Framers were men focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth.").

An individual's reasonable expectation of privacy does not vanish because technological advances permit intrusions of a nature or scope not previously available. "[T]here are [limits] upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Thus, the use of a thermal imaging device to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search – . . . ," *id*. at 34 (internal citations omitted), and, if warrantless, is presumptively unreasonable, *id*. at 40. These limitations were again recognized recently in *United States v. Jones*, 132 S. Ct. 945 (2012), where attachment of a Global Positioning System (GPS) tracking device to an individual's vehicle and its use to monitor the vehicle's movements for four weeks was held to be a search. Although the opinion of the Court rested on the government's physical intrusion to install the device for the purpose of obtaining information, *see* 132 S. Ct. at 949-951, a concurrence by Justice Alito (joined by Justices Ginsburg, Breyer, and Kagan) found that the government's actions in long-term GPS tracking also violated the defendant's reasonable expectation of privacy. Justice Alito explained that for

common drug offenses, like the offense in *Jones*, "society's expectation has been that law enforcement agents and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id*. at 964. Justice Sotomayor agreed with Justice Alito in a separate concurrence, concluding that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id*. at 955. In addition, Justice Sotomayor suggested that the intrusiveness of GPS surveillance of any duration might raise Fourth Amendment concerns because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id*. at 955-956.

Like GPS surveillance, searches of cell phones and other personal electronic devices can generate a wealth of detail about a person's associations, personal information, and private life that would have been wholly unattainable from a search of one's person in the pre-electronic age. The government maintains that law enforcement officers can access that store of private, personal information without a warrant simply because someone is carrying a cell phone or other personal electronic device at the time of her arrest. Mr. Wurie maintains that the government's position misinterprets the scope, history, and purposes of the search-incident-to-arrest exception to

the warrant requirement and should be rejected by this Court.

B. The Search of the Contents of a Cell Phone Is Not Within the Scope of the General Search-Incident-to-Arrest Exception to the Warrant Requirement; It Is Not Supported by Either of the Two Justifications of Officer Safety and Prevention of the Destruction of Evidence

The search-incident-to-arrest doctrine is an exception to the "basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (citation omitted). The exception "derives from interests in officer safety and evidence preservation that are typically implicated in arrest situations." *Id.* The government both seeks to expand the basis for the exception, as explained in *Chimel v. California*, 395 U.S. 752 (1969), and misreads *United States v. Robinson*, 414 U.S. 218 (1973), which neither abandons nor expands on those purposes. The government further seeks to extend *Gant* to a context other than automobiles. This Court should reject the government's arguments.

1. *Chimel v. California* Defined the Constitutionally Permissible Scope of a Search Incident to Arrest

The permissible scope of a search incident to arrest fluctuated for the first half of the twentieth century.[3] In *Chimel*, the Court noted it had "been far from consistent" in its interpretation of the constitutionally permissible scope of a search incident to arrest and revisited the constitutionally permissible scope of such a search in light of "the background and purpose of the Fourth Amendment." 395 U.S. at 760 (1969). The Court concluded that it was constitutionally

---

[3] *See*, *e.g.*, *Weeks v. United States*, 232 U.S. 383 (1914) (warrantless search of arrestee's home impermissible where arrest took place elsewhere); *Agnello v. United States*, 269 U.S. 20 (1925) (same); *Marron v. United States*, 275 U.S. 192 (1927) (warrantless search of all parts, including closets, of premises on which arrestee located and in which criminal enterprise was located permissible); *Go-Bart Importing Co. v. United States*, 282 U.S. 344 (1931) (warrantless, general, unlimited search of office in which arrestee located impermissible); *United States v. Lefkowitz*, 285 U.S. 452 (1932) (same); *Harris v. United States*, 331 U.S. 145 (1947) (warrantless search of entire four-room apartment in which arrestee located permissible), *overruled by Chimel v. California*, 395 U.S. 752 (1969) (warrantless search that goes beyond arrestee's person and area from which he might obtain weapon or destructible evidence impermissible); *Trupiano v. United States*, 334 U.S. 699 (1948) (warrantless seizure of illegal still being operated by arrestee at time of arrest impermissible where agents had ample opportunity beforehand to obtain search warrant); *United States v. Rabinowitz*, 339 U.S. 56 (1950) (warrantless search of office in which arrestee located, including desk, safe and file cabinets, permissible), *overruled by Chimel v. California*, 395 U.S. 752 (1969).

reasonable to search the person of an arrestee "in order to remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape" and "in order to prevent . . . concealment or destruction [of evidence]." *Id*. at 763. The Court held further that "the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule." *Id.*

In the forty years since *Chimel*, the Court has not wavered in its articulation of the limits placed on the search-incident-to-arrest exception to the warrant requirement. For example, this Court recently reaffirmed *Chimel*'s limiting principles when it observed, "[t]hat limitation, which continues to define the boundaries of the exception, ensures that the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy." *Arizona v. Gant*, 556 U.S. 332, 339 (2009).[4] *See also Virginia v. Moore*, 553 U.S. 164, 176 (2008) (stating that "officers may perform searches incident to arrest to ensure their safety and safeguard evidence.").

[4] In *Gant*, this Court also held that "circumstances unique to the automobile context justify a search incident to arrest when it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle." 556 U.S. at 335.

2. *United States v. Robinson* Adhered to *Chimel*'s Limitations

The government relies heavily on *United States v. Robinson*, 414 U.S. 218 (1973), *see* U.S. Br. 17-29, but *Robinson* cannot carry the weight the government places on it. In *Robinson*, the Court addressed the scope of the search-incident-to-arrest exception in the context of the search of a "crumpled up cigarette package" seized from the coat pocket of a person arrested for operating a motor vehicle after revocation of his operator's permit. After feeling objects in the package he could not identify, an officer opened it and found capsules containing what turned out to be heroin. 414 U.S. at 223-224.

The court of appeals had framed the relevant question as "whether and under what circumstances, an arresting officer may conduct a *full* search of the person incident to a lawful arrest for violation of a mere motor vehicle regulation." *United States v. Robinson*, 471 F.2d 1082, 1090 (D.C. Cir. 1972) (en banc) (emphasis in original). The circuit court concluded that under these circumstances, the scope of a permissible search incident to arrest was more limited than that authorized in *Chimel*. It held that, in the context of routine traffic arrests where the officer intends only to issue a violation, the only search permitted is the type of limited patdown for weapons authorized by *Terry v. Ohio*, 392 U.S. 1 (1968), based upon special facts or circumstances providing reasonable grounds to believe the person is armed and dangerous. 471 F.2d at 1097. Where the officer was

required to take the motor vehicle violator into custody, "a limited *frisk* of the suspect's outer clothing in order to remove any weapons the suspect may have in his possession" was permissible. 471 F.2d at 1098 (emphasis in original).

This Court rejected the appellate court's limitation of a search incident to arrest to a *Terry*-based weapons frisk. *Robinson*, 414 U.S. at 227-229. Recognizing that "[v]irtually all of the statements of this Court affirming the existence of an unqualified authority to search incident to a lawful arrest are dicta," *id.* at 230, the Court examined the "sparse" authorities addressing the issue prior to 1914. *Id*. It found the "sketchy" authorities "tend[ed] to support the broad statement of the authority to search incident to arrest found in the successive decisions of this Court, rather than the restrictive one which was applied by the Court of Appeals in this case," *id*. at 232, 232-233. Essentially, the Court held that a *Chimel*-type search is permissible whenever a defendant is arrested, even if that arrest is for a routine traffic offense. Accordingly, the search of the cigarette package was constitutionally permissible.

The Court further held that the right to search incident to arrest did not require a case-by-case adjudication of whether "one of the reasons supporting the authority for a search of the person incident to a lawful arrest" was present. The fact of lawful arrest justified a full search of the person as an exception to the warrant requirement and a reasonable search. *Id*. at 235. The full search authorized was contrasted

with the limited search – a frisk for weapons – permitted by *Terry*. *Id*. at 232-234.

Critically, however, in approving a full search of the person, the Court did not question, change, expand, or dispense with the justifications for a search incident to arrest – officer safety and the prevention of the concealment or destruction of evidence – or suggest that different justifications might exist in this specific context. Indeed, some of the early cases in which the Court found a broad statement of authority to search incident to arrest described those searches as based on a need for preservation of evidence. *See Dillon v. O'Brien*, 16 Cox C.C. 245, 250 (Exch. Ireland, 1887) ("[T]he interest of the State . . . necessarily extends, as well to the preservation of material evidence of his guilt or innocence. . . ."); *Holker v. Hennessey*, 42 S.W. 1090, 1093 (Mo. 1897) ("[U]nless the arresting officer has the authority [to search a prisoner] immediately on making the arrest, all evidences of crime and of identification of the criminal might be destroyed before the prisoner could be taken to the magistrate.").

Robinson quoted *Chimel*'s application of the officer-safety and prevention-of-evidence-destruction justifications to the search of the person incident to arrest and reiterated that "[t]he justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial." *Id*. at 226, 234. Contrary to the

government's contention here, U.S. Br. 17, the Court did not suggest that those justifications were inapplicable to searches of the person and only applied to searches of areas within the arrestee's immediate control not on his person. They apply with equal force to the search of the contents of a cell phone as part of a search incident to arrest of the person.

3. The Limited Expansion of the Scope of a Constitutionally Permissible Search Incident to Arrest in *Arizona v. Gant* Should Remain Limited to Recently Vacated Automobiles

Just as the government's reliance on *Robinson* is misplaced, so, to, is its reliance on *Arizona v. Gant*, 556 U.S. 332 (2009). U.S. Br. 44-49. In *Gant*, this Court found that "circumstances unique to the automobile context" justified a somewhat broader application of the search-incident-to-arrest doctrine in the limited set of cases where an automobile was recently vacated by an arrestee. In such cases, police may conduct a search based on a reasonable belief that evidence of the offense of arrest might be found in the recently vacated vehicle. *Id*. at 335.

This narrow expansion of the authority to search incident to arrest should remain limited to the automobile context. This Court has repeatedly asserted that there is a reduced expectation of privacy associated with automobiles for a variety of reasons. Automobiles travel on public thoroughfares. They seldom

serve as a repository of personal effects. They are subject to pervasive governmental regulation and control. They are at risk for traffic accidents that may expose all of their contents to public view. *See*, *e.g.*, *Wyoming v. Houghton*, 526 U.S. 295, 303 (1999). In addition, their mobility has been held to justify an exception to the warrant requirement where there is probable cause to believe evidence of crime will be found inside. *Carroll v. United States*, 267 U.S. 132 (1925). Adding these factors to the reduced expectation of privacy engendered by an arrest may justify the search of a vehicle simply for general evidence of the offense of arrest. Without those added factors, the reduced expectation of privacy engendered by an arrest alone does not support expanding the scope of a warrantless search incident to arrest outside the automobile context.

The government's suggestion that the same framework applicable to searches of automobiles should apply to searches of personal electronic devices, U.S. Br. 45-49, is misplaced because these automobile considerations do not apply to cell phones. The two situations are not comparable. There are no mobility concerns associated with a cell phone seized by the police. The use of cell phones is not subject to government control in the same way motor vehicles are. Although many cell phones are used in public, many are also used in the most private of places, like bedrooms and bathrooms. There is, moreover, a far greater expectation of privacy in the vast array of personal, private information contained in a cell phone than there is in an automobile.

Thus, the government's analogy to the search of an automobile fails and reason to believe evidence of the crime of arrest can be found by searching the phone does not justify ignoring the warrant requirement. Once the police have seized a cell phone, the justification for a search for evidence of an offense should be submitted to a neutral magistrate for a determination of probable cause for a search and the imposition of limits on any search authorized. Outside the context of the search of an automobile incident to the arrest of its occupant, this Court should continue to limit application of the search-incident-to-arrest exception only to those searches justified by the twin concerns of officer safety and the prevention of the destruction of evidence.

C. The Government's Contention That the Scope of a Search of the Person Incident to Arrest Is Not Limited to the Type of Search Necessary for Protecting Officer Safety or Preventing Destruction of Evidence Is Based on a Flawed Interpretation of This Court's Jurisprudence and a Selective Reading of History

The government seeks to avoid the lack of any connection between the warrantless search of the information contained in a cell phone seized from a defendant's person and the two *Chimel* justifications of officer safety and evidence preservation in two ways. First, the government argues that these justifications are limited to the search of "the area around the arrestee." It then argues that, as to the search of the

person of an arrestee, history and the reduced expectation of privacy after a lawful arrest mean that there are no limits and *Chimel* does not apply. Police have "full authority" to search the person of an arrestee and any and all items found on the person. U.S. Br. 13. These arguments rely on an incorrect reading of *Robinson*, a selective reading of history, and an undue emphasis on the arrestee's reduced expectation of privacy.

As discussed above, *supra* section B.2, *Robinson* did not limit application of the *Chimel* justifications for a search incident to arrest to the search of the area around the arrestee. It reaffirmed the applicability of the officer-safety and prevention-of-evidence-destruction justifications to the search of the person incident to arrest, but created a presumption that these justifications applied after a lawful arrest so that courts need not make case-by-case determinations that the government either had or had not established the presence of those justifications. This holding does not, as the government maintains, resolve this case. U.S. Br. 17.

It may be reasonable to assume that, in general, an arrestee may have a weapon hidden in small or unlikely packages or have evidence she would attempt to destroy and, therefore, to allow an officer to search for and seize such items after any arrest. Indeed, while the government asserts that the cigarette package in *Robinson* could not have reasonably been thought to contain a weapon, U.S. Br. 24, four judges on the D.C. Circuit Court found just such a

possibility. *See United States v. Robinson*, 471 F.2d 1082, 1114, 1117-1118 (D.C. Cir. 1972) (en banc) (Wilkey, Tamm, MacKinnon and Robb, JJ., dissenting) (discussing possibility of razor blade, and noting .22 caliber pistol made from small aluminum tube concealed in cigarette package). Arrestees may have a variety of small weapons. Arrestees found to have knives, scissors, razor blades and glass shards concealed on their person at a jail, *see Florence v. Board of Chosen Freeholders*, 132 S. Ct. 1510, 1519 (2012), are likely to have had them on their person at the time of their arrest.

The reasonableness of a presumption does not, however, eliminate the need for a court to evaluate whether a discrete category or type of search conducted subsequent to an arrest is not generally supported by the justifications of officer safety and prevention of evidence destruction. If, for example, an officer seized a labeled safe deposit box key while conducting a search incident to arrest and took that key to the bank, a warrantless search of the box using that key could not be justified as incident to arrest. We would expect the officer to obtain a warrant. In the same way, while it might be reasonable for an officer to remove the battery pack of a phone to search for any concealed items like razor blades, a search of the electronic contents of the phone cannot be justified on the same basis.

More importantly, a cell phone or other personal electronic device is not simply another closed container like the cigarette package in *Robinson*. It holds

digital data, not physical objects. It can be, and often is, a virtually limitless portal to an individual's private and personal information and thoughts, both on the device and stored elsewhere. There are no discrete boundaries to its contents. As the First Circuit and other courts have recognized, the container analogy is flawed, for it ignores both qualitative and quantitative differences. *See Wurie*, 728 F.3d at 9; *United States v. Wicks*, 73 M.J. 93, 102 (C.A.A.F. 2014); *Smallwood v. State*, 113 So. 3d 724, 736 (Fla. 2013); *United States v. Mayo*, 2013 WL 5945802, at *6-*10 (D. Vt. Nov. 6, 2013); *State v. Smith*, 920 N.E.2d 949, 954 (Ohio 2009).

Nor does history clearly support an unlimited search of an arrested person merely for purposes of general evidence-gathering. In *Thornton v. United States*, 541 U.S. 615, 629-631 (2004) (Scalia, J., concurring), Justice Scalia described the early history of the right to search the person arrested as supporting differing propositions. He noted that while some pre-*Chimel* case law justified searches incident to arrest on a more general interest in gathering evidence relevant to the crime of arrest, "*Chimel*'s narrower focus on concealment or destruction of evidence also has historical support."

Preventing the destruction of evidence requires the authority to search incident to arrest and to seize items that may be destroyed. Evidence can only be preserved if it is located and seized. But granting police the right to seize items from the person incident to arrest without a warrant does not require

authorizing them to search all items taken into custody without a warrant. *See*, *e.g.*, *United States v. Van Leeuwen*, 397 U.S. 249, 250 (1970) (approving detention of package pending application for search warrant). The First Circuit here did not hold, and Mr. Wurie does not argue, that his cell phone was impermissibly seized and secured by the officers. What the First Circuit correctly held is that the warrantless search of the private information in Mr. Wurie's phone was beyond the scope of a constitutionally permissible search incident to arrest and therefore violated the Fourth Amendment.

The government's contention that the reduced expectation of privacy arising from arrest justifies any and all searches of the person incident to arrest, including the warrantless search of the information in a cell phone possessed by the arrestee, gives that factor undue weight, to the point of entirely eliminating any privacy expectation. But the mere fact of arrest does not eliminate the arrestee's reasonable expectation of privacy and justify every post-arrest search as one incident to arrest. As this Court stated just last Term when considering the reasonableness under the Fourth Amendment of a post-arrest cheek swab to obtain a DNA sample, "This is not to suggest that *any* search is acceptable *solely* because a person is in custody." *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013) (emphases added). *See also United States v. Edwards*, 415 U.S. 800, 809 (1974) (stating that "we do not conclude that the Warrant Clause of the Fourth Amendment is never applicable to postarrest

seizures of the effects of an arrestee."). Notwithstanding the reduced expectation of privacy following a lawful arrest, this Court did not, in *Missouri v. McNeely*, 133 S. Ct. 1552 (2013), analyze the constitutionality of a blood draw from a person arrested for operating under the influence of alcohol under the search-incident-to-arrest exception.

The government argues that *United States v. Edwards*, 415 U.S. 800 (1974) (upholding seizure and search of clothing taken from arrestee at jail the morning after his arrest), "underscored" that the authority to search the person of an arrestee incident to arrest "rests principally" on a reduced expectation of privacy. U.S. Br. 19. However, in addition to searches incident to arrest, the Court in *Edwards* also discussed the inventory rationale and the jailer's interest in searching a person being incarcerated as justifications for the seizure and search. 415 U.S. at 804-805 & n.6. It also noted the reasonableness of the police action "particularly in view of the existence of probable cause linking the clothes to the crime." *Id.* at 806. Nor did the defendant challenge the subsequent search of his clothing; he challenged only its seizure. *Id.* at 802.

Even though an arrestee's expectation of privacy is diminished (but not eliminated), the constitutionality of post-arrest warrantless searches must still be determined by weighing particular governmental interests against the reduced expectation of privacy and the nature of the intrusion, as this Court has done in a number of cases. In the context of the

incident-to-arrest search, officer safety and the prevention of evidence destruction must be weighed against the reduced expectation of privacy in determining whether a particular type or category of post-arrest search is constitutionally permissible. Other balances are applied in evaluating the applicability of other exceptions to the warrant requirement.

In *McNeely*, for example, the Court analyzed the constitutionality of the blood draw under the exigent circumstances exception. It rejected the state's argument that a warrantless blood draw was categorically reasonable because the "inherently evanescent" nature of blood alcohol concentration evidence always gives rise to exigent circumstances. 133 S. Ct. at 1560. *See also Illinois v. Lafayette*, 462 U.S. 640, 646-647 (1983) (search of defendant's shoulder bag at police station following his arrest was justified by interests of inventory search of property of person to be jailed); *Florence v. Board of Chosen Freeholders*, 132 S. Ct. 1510 (2012) (visually invasive suspicionless post-arrest strip searches at jail prior to placement in general population justified by interests of institutional security and order); *Maryland v. King*, 133 S. Ct. 1958, 1974 (2013) (post-arrest taking of DNA pursuant to statute justified by government interest in identity, deemed relevant to custody decisions and "with consequences for every stage of the criminal process"). In no case post-*Chimel* has this Court adopted the blanket expansion of the search-incident-to-arrest exception advocated by the government in this case.

Here, while Mr. Wurie's reduced expectation of privacy may have justified searching his person and seizing his cell phone from his control to prevent the potential destruction of evidence, it did not justify the warrantless *search* of the personal and private information on that device. This Court did not in *Robinson*, and should not now, untether the scope of a constitutionally reasonable search incident to arrest of the person from its twin justifications of officer safety and the prevention of evidence destruction. It did not, and should not now, authorize a search of limitless scope of any item found on the person.

Such an expansion is particularly unwarranted with respect to cell phones and other personal electronic devices found on the person. Advances in technology have given people the ability to put the contents of their desk drawers and file cabinets in their pocket. The deeply personal and private nature of the information contained in those devices, as well as the sheer amount of that information, undermines the government's claim that their search can be justified by the reduced expectation of privacy accompanying an arrest. A person arrested for failing to wear a seatbelt, *see Atwater v. City of Lago Vista*, 532 U.S. 318 (2001), should not be subject to having her private life and associations laid bare by granting police unfettered access to the complete contents of her cell phone.

The First Circuit examined the nature of the cell phone and the individual's privacy interests in the information it contains, and using the principles set

out in *Chimel* and applied in this Court's subsequent search-incident-to-arrest jurisprudence, concluded that the warrantless search of the information contained in that device could not be justified by a need for either officer safety or preventing the destruction of evidence. Rather, while officers could seize and secure the phone, they had to get a warrant to search its contents. This Court should reach the same conclusion.

D. The Warrantless Search of the Information in a Cell Phone Is Not Justified by Concerns About Protecting Officer Safety or Preventing Destruction of Evidence

The government alternatively maintains that the search of Mr. Wurie's cell phone was justifiable under the limitations imposed by *Chimel* because the search was necessary to protect officer safety, U.S. Br. 41-42, and because the information in the device was subject to destruction or concealment after it was taken into police custody, U.S. Br. 33-41. Neither of these contentions support a warrantlesss search incident to arrest.

1. Protecting Officer Safety

Chimel's officer safety justification for the warrantless search incident to arrest is the need to seize weapons or items that the arrestee may use to assault an officer. 395 U.S. at 763-764. Plainly, a cell phone or other personal electronic device poses no

such threat. Yet, the government hypothesizes a need to search a cell phone's contents on the highly unlikely possibility that "reviewing the recent calls and text messages . . . can alert the officers that confederates are headed to the scene of the arrest and that they should take safety precautions or call for backup." U.S. Br. 41. This claim, for which the government provides no support, rests on several unfounded assumptions: that an arrestee has confederates; that the confederates are armed with weapons and on their way in sufficient numbers to pose a threat to law enforcement on the scene; and that the confederates have announced their intent in text messages or calls. This hypothetical scenario falls far from the threat of an arrestee with weapons facing the arresting officer(s) described in *Chimel*. *See* 397 U.S. at 762-763.

If, in fact, that confluence of factors arises in a particular case, it is a scenario that can be addressed through the exigent circumstances exception to the warrant requirement. Claims of officer security are not exempt from scrutiny. Indeed, in *Bailey v. United States*, 133 S. Ct. 1031 (2013), this Court rejected claims of officer safety and search efficiency as justifying expansion of the *Summers*[5] rule authorizing officers executing a search warrant to detain the occupants of premises being searched to allow police to detain people some distance from the house. Here,

[5] *Michigan v. Summers*, 452 U.S. 692 (1981).

there is no justification for adopting a blanket rule that officer safety is threatened by seizing and securing a cell phone rather than searching it.

2. Preventing Destruction of Evidence

The government argues that the availability of passwords, automatic locking, erasure, encryption, and remote wiping all justify a warrantless search incident to arrest to prevent the destruction of evidence. U.S. Br. 33-41. This parade of horribles is overblown.

The government begins by claiming that there are potential difficulties in overcoming a password lock used to secure information on a cell phone or other personal electronic device from access by others. U.S. Br. 34-37. However, it provides no information on how often such difficulties have been encountered, much less have actually resulted in the destruction of evidence. Further, there are forensic tools and assistance to obtain password protected information. *See*, *e.g.*, *United States v. Mathis*, 2013 WL 869511, at *1 (M.D. Fla. Feb. 19, 2013) (warrant for forensic examination of phone "to extract hidden, erased, or password-protected information"); *United States v. Brown*, 2013 WL 1185223, at *2 (E.D. Ky. Mar. 20, 2013) (provision of assistance from Apple to unlock password protected phone). The same issues arise in connection with the search of computers and other devices for evidence of child pornography. Yet warrants are routinely sought for such searches. *See*, *e.g.*,

United States v. Seiver, 692 F.3d 774, 775 (7th Cir. 2012) (discussing "staleness" and computer searches and listing examples of the "*very* large number of cases" concerning probable cause in a warrant to search a computer for child pornography) (emphasis in original). Finally, the government should not be allowed to transform the step an individual takes to safeguard the privacy of her information into a justification for eroding the protections of the Fourth Amendment.

The government next expresses concern over remote wiping, the erasing of information from a device by a third party. U.S. Br. 37-40. As the First Circuit explained, the use of a Faraday bag or enclosure – "a relatively inexpensive device 'formed by conducting material that shields the interior from external electromagnetic radiation'" – can address any danger of remote wiping. *Wurie*, 728 F.3d at 11. *See also United States v. Smith*, 715 F.3d 1110, 1114 (8th Cir. 2013) (describing use of Faraday bag and airplane mode to prevent remote wiping); Adam Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Farady Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 Wm. & Mary Bill Rts. J. 601 (2013). Turning the phone off and removing the battery can also prevent remote wiping. *United States v. Dixon*, ___ F. Supp. 2d ___, 2013 WL 6055396, at *2 (N.D. Ga. Nov. 15, 2013).

Copying the device's contents to another device without reviewing the information to preserve it pending a warrant authorizing a search is another option.

Wurie, 728 F.3d at 11; *United States v. Aispuro*, 2013 WL 3820017, at *14 (D. Kan. Jul. 24, 2013) (police copied contents of cell phone to storage device before later warrantless search; warrantless search held not to be within scope of search incident to arrest). Law enforcement has developed many methods for doing this. The FBI has cell phone investigative kiosks available at 84 offices around the country and portable kiosks available at 81 locations; these kiosks "allow users to extract data from a cell phone, put it into a report, and burn the report to a CD or DVD in as little as 30 minutes." U.S. Department of Justice, Federal Bureau of Investigation, "Cell Phone Investigative Kiosks," *available at* http://www.rcfl.gov/DSP_P_CellKiosk.cfm. The Regional Computer Forensics Laboratory Program, a program overseen by the FBI and executives from law enforcement agencies participating in a specific laboratory, also has cell phone investigative kiosks. U.S. Department of Justice, Federal Bureau of Investigation, "RCFLP Annual Report for FY 2012," *available at* http://www.rcfl.gov/DSP_N_annualReport.cfm. Use of these kiosks would provide a means of evidence preservation pending application for a warrant.

Some states already implement such practices. Vermont DEA Task Force Agents "used a Cellebrite machine to download the contents of Mayo's phones, including the cell phone number, a contacts list, text messages, call records, and assorted images." That machine "is a device used by law enforcement to extract data from cell phones and other digital devices."

United States v. Mayo, 2013 WL 5945802, at *2 (D. Vt. Nov. 6, 2013). *See also Dixon*, 2013 WL 6055396, at *2 (in case involving use of Cellebrite machine, holding that download of data was unconstitutional search, not within scope of search incident to arrest, where information reviewed without a warrant). According to an official statement from the Michigan State Police, "[d]ata extraction devices are commercially available and are routinely utilized by mobile communication device vendors nationwide to transmit data from one device to another. . . ." Michigan State Police, "Official Statement: Use of Cell Phone Data Extraction Devices," April 20, 2011, *available at* http://www.michigan.gov/msp/0,1607,7-123-1586-254783--,00.html. These devices could also preserve cell phone information pending a warrant.

Notwithstanding the government's assertions of the inadequacy of such protective measures, some jurisdictions preclude the warrantless search of cell phones or allow it only with consent or exigent circumstances. "It is Vermont state law enforcement's policy to obtain consent or a warrant for all cell phone searches according to the Government's witnesses." *Mayo*, 2013 WL 5945802, at *2. Similarly, "[t]he MSP [Michigan State Police] only uses the DEDs [data extraction devices] if a search warrant has been obtained or if the person possessing the mobile device gives consent." Michigan State Police, "Official Statement: Use of Cell Phone Data Extraction Devices," April 20, 2011, *available at* http://www.michigan.gov/msp/0,1607,7-123-1586-254783--,00.html. The District

Attorney for Westchester County, New York, provided the following advice to the law enforcement community concerning computer devices: "data which is not visible on an open screen or computer, including a cell phone, is not evidence in plain view. A search for stored data such as contacts and phone numbers in cell phones must be preceded by a warrant or supported by consent or exigent circumstances permitting a warrantless search." Janet DiFiore, District Attorney, Westchester County, "The Criminal Law News," Vol. 1, No. 2, p.7 (Feb. 2007).

Finally, while preservation options may not be without cost or effort, those costs cannot override an individual's interest in protecting her private information against unwarranted government intrusion. The law enforcement interest in investigating and gathering evidence of crime is undeniably a compelling one, but a general interest in effective law enforcement cannot be elevated over citizens' interests in the protection of their constitutional rights, including their Fourth Amendment rights. *See*, *e.g.*, *Georgia v. Randolph*, 547 U.S. 103, 115 n.5 (2006) ("A generalized interest in expedient law enforcement cannot, without more, justify a warrantless search.").

"[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." *Mincey v. Arizona*, 437 U.S. 385, 393 (1978); *Gant*, 556 U.S. at 349 (quoting *Mincey*). The Court has relied on that principle in refusing a murder scene exception, or an arson investigation exception, or a firearms exception to the

Fourth Amendment, all argued to be permissible means to facilitate law enforcement efficiency. *Flippo v. West Virginia*, 528 U.S. 11 (1979); *Mincey v. Arizona*, 437 U.S. 385 (1978) (murder scene); *Michigan v. Clifford*, 464 U.S. 287 (1984); *Michigan v. Tyler*, 436 U.S. 499 (1978) (arson investigation); *Florida v. J.L.*, 529 U.S. 266, 272 (2000) (firearms). As the First Circuit stated: "[W]arrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant's crime of arrest – or other, as yet undiscovered crimes – without having to secure a warrant. We find nothing in the Supreme Court's search-incident-to-arrest jurisprudence that sanctions such a 'general evidence-gathering search.'" *Wurie*, 728 F.3d at 13 (internal citation omitted). This Court should continue to reject sanctioning a general evidence-gathering search under the search-incident-to-arrest exception and refuse to permit interests of law enforcement efficiency to override the individual's right to the protections of the Fourth Amendment. Instead, the Court should require a determination of probable cause by a neutral magistrate before the vast array of personal information in cell phones and other personal electronic devices is subject to search.

E. This Court Should Reject the Government's Suggestion to Redefine the Scope of the Search of a Cell Phone Incident to Arrest

The government alternatively asks this Court to redefine the scope of a search of a cell phone incident to arrest, contending that it is constitutionally

reasonable to permit the warrantless search of a cell phone seized from an arrestee for evidence of crime, identifying arrestees and protecting officers. It purports to impose limitations by suggesting that a search for such information be permitted only in "every area of a cell phone's contents" where officers have an objectively reasonable basis to believe such information would be found. U.S. Br. 49-54. This proposal is in reality a request for authorization to conduct a virtually limitless warrantless search.

A search for the discovery of evidence of crime imposes no constraints. Call logs, texts, notes and memos, contact lists, photos – all could be said to be areas that could contain such evidence. No area of the phone would be off-limits. Nor is there any justification for eviscerating the probable cause and warrant requirements of the Fourth Amendment simply to allow law enforcement officers to search for evidence of crime.

The suggestion that the need to confirm the identity of an arrestee generally justifies a warrantless search of a cell phone seized incident to arrest should also be rejected as another effort to make an end run around the probable cause and warrant requirements of the Fourth Amendment. There are reliable ways of confirming identity if identity is, in fact, an issue. *See*, *e.g.*, *King,* 133 S. Ct. at 1975-1976. A cell phone search is not among them, for there is no way to determine whether a person is carrying a phone she owns and has registered in her own name or a phone belonging to someone else, and examining

information on a phone seized from a person will not tell the officer whether the person has used false information in securing phone service. Because any need to confirm identity will not be achieved by searching a phone seized incident to arrest, this rationale should not serve to justify a warrantless search.

Finally, as discussed previously, *see supra* section D.1, the cell phone poses no general threat to officer safety and provides no justification for general approval of a warrantless search. In short, none of the justifications offered for a warrantless search of a cell phone seized incident to arrest support a determination that a warrantless search for those purposes is constitutionally reasonable. Police officers should be allowed to seize and secure a cell phone incident to arrest and, unless some other exception to the warrant requirement is shown to be applicable, must comply with the probable cause and warrant requirements of the Fourth Amendment.

F. Call Logs Are Not Exempt From the Warrant Requirement

Finally, the government argues that officers should always be allowed to search call logs because this Court held in *Smith v. Maryland*, 442 U.S. 735 (1975), that an individual has no legitimate expectation of privacy in his dialed phone numbers. U.S. Br. 54. This expansive reading of *Smith* is unwarranted and constitutionally dubious as applied to records on an individual's cell phone for several reasons.

First, *Smith's* third-party doctrine does not apply to such records in the possession of the user, who is not a third party. As the government acknowledges, an individual does have a property interest in his cell phone, U.S. Br. 54, and therefore in the information on that phone, including its call logs. "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 35 n.2 (2001).[6]

Second, unlike the pen register involved in *Smith*, which recorded only outgoing phone numbers and did not indicate whether a call was completed, a cell phone call log may indicate not only whether a call was completed, but also contain records of incoming calls, thereby revealing more information than phone company pen register records. The call log also goes well beyond the limited pen register information of numbers dialed by including associational information created by the user of the cell phone. It may link a name, a nickname, or a place with a number. It may identify a number by relationship such as "psychiatrist," "partner," or "Mom." Indeed, it was just

[6] In *United States v. Jones*, Justice Sotomayor suggested "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties[,]" describing this approach as "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

such associational information – the phone number associated with the descriptive "my house" – that the police officers searched for in this case.

The government's proposed broad rule also ignores the fact that the pen register information upheld in *Smith* was data obtained on a single day for a specific purpose – to see if the defendant was the person making threatening and obscene phone calls to a woman the caller had robbed. The government's proposed rule places no limit on law enforcement searching of call logs. Yet, the associational information to be gleaned from call logs may be enhanced if the logs are examined for an extensive period of time, providing patterns of calling that can be combined with other information to create a profile of the cell phone user's life.

Moreover, the government can no longer simply ask the phone company to install a pen register. Congress now requires law enforcement officers to obtain a court order, and limits the use of the pen register to 60 days with procedures for applying for an extension. *See* 18 U.S.C. §3121 *et seq*. While a statutory protection does not define constitutional protections, it is relevant to a reasonable societal expectation of privacy.

Nor is the government's call-record exception workable in the field. Officers searching cell phone call logs incident to arrest cannot be expected to know how to access only a call log on each make and model of cell phone. Efforts to locate a call log may well

expose protected information such as photographs or a listing of applications installed, which may, in turn, reveal personal or other associational information.

G. A Seize-and-Secure Policy Strikes the Proper Balance Between Law Enforcement Interests and the Individual's Interest in Freedom From Unreasonable Searches and Seizures With a Rule Easily Administered in the Field

The government contends that excluding the search of the information in cell phones and other personal electronic devices from the scope of a search incident to arrest will necessitate some item-by-item judgment that is difficult to administer in the field. U.S. Br. 26-27. This suggestion is unfounded. The seize-and-secure line drawn by the First Circuit, which this Court should affirm, is clear and easy for officers in the field to administer. Pursuant to this rule, the information in a cell phone or other personal electronic device may not be searched without a warrant incident to arrest. It is a categorical rule that does not require item-by-item assessment of a particular phone or device. Nor does it preclude the application of some other exception to the warrant requirement, such as exigent circumstances. The applicability of that, or any other exception, would have to be judged by the officer in the field and, if challenged, evaluated by a court, as it must be today.

The government's fear that recognizing the qualitative and quantitative differences between personal

electronic devices and other items people carry with them outside their homes will "destabilize" what it characterizes as a "settled framework" for the post-*Robinson* warrantless search of personal items such as pagers, wallets, purses, address books and briefcases, U.S. Br. 27-28, is misplaced for at least three reasons. First, a seize-and-secure rule for cell phones and other personal electronic devices does not affect the framework for analyzing when items which may contain weapons or evidence an arrestee may attempt to destroy may be searched incident to arrest. Second, the government ignores the fact that this Court has never held that items such as address books and papers may be read without a warrant incident to arrest pursuant to *Robinson*.

Third, the government fails to address the varied analyses in some of the lower court cases it cites as illustrative of a "settled" framework. *See* U.S. Br. 27-28. Some have simply cited *Robinson* as justification for the seizure of items such as wallets and address books. *See United States v. Watson*, 669 F.2d 1374, 1383-1384 (11th Cir. 1982); *United States v. Diaz-Lizaraza*, 981 F.2d 1216, 1223 (11th Cir. 1993). *United States v. Ortiz*, 84 F.3d 977 (7th Cir. 1996), emphasized the ephemeral nature of the information contained in a pager and the need to avoid loss of evidence, thereby tying its analysis to the *Chimel* justifications. Before concluding that agents "had ample justification for searching [the defendant], examining his wallet and seizing the contraband concealed in it," the court in *United States v.*

Uricoechea-Cassallas, 946 F.2d 162, 165-166 (1st Cir. 1991), described the justifications of a search incident to arrest as preserving evidence and seizing destructible contraband. The court also found the search of the defendant to be a permissible border or customs search. Accordingly, Mr. Wurie suggests that there is no "settled framework" for searching personal information contained in other items to be disturbed by holding that law enforcement may not search the contents of cell phones or other personal electronic devices pursuant to the incident-to-arrest exception to the warrant requirement.

The government acknowledges that even under the virtually unlimited scope it proposes, the search-incident-to-arrest exception does not justify using a seized cell phone to access files or information stored elsewhere (the internet "cloud" or a home computer). U.S. Br. 44. However, an officer searching an electronic device simply cannot know the location of the information accessed by pushing buttons on the innumerable types and models of devices. The impossibility of enforcing the concededly required limitation also counsels requiring a warrant to search for information on a cell phone or other device. Unlike the government's rule, the First Circuit's seize-and-secure line is readily administrable in the field. Equipped with this rule, an officer can know the precise parameters of his authority.

CONCLUSION

The government conducted a warrantless investigatory search of Mr. Wurie's cell phone subsequent to his arrest. It maintains that the search was permitted under the search-incident-to-arrest exception to the warrant requirement. However, as the First Circuit held, the search of the information contained in a cell phone is not of a type generally justified by either officer safety or the prevention of the destruction of evidence, the two justifications for a constitutionally permissible search incident to arrest. The First Circuit was correct. For the foregoing reasons the judgment of the court of appeals should be affirmed.

Respectfully submitted,

JUDITH H. MIZNER
Counsel of Record
FEDERAL DEFENDER OFFICE
51 Sleeper Street, 5th Floor
Boston, MA 02210
(617) 223-8061
Judith_Mizner@fd.org