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 OF THE NATIONAL ASSOCIATION OF FEDERAL DEFENDERS AND THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

SARAH S. GANNETT &
DANIEL KAPLAN, CO-CHAIRS
KEITH M. DONOGHUE,
MEMBER
AMICUS COMMITTEE
NAT'L ASS'N OF FEDERAL
DEFENDERS
601 Walnut St., Ste. 540W
Philadelphia, PA 19106

MASON C. CLUTTER
NAT'L ASS'N OF CRIMINAL
DEFENSE LAWYERS
1660 L St., NW
Washington, DC 20036

JEFFREY T. GREEN*
JACQUELINE G. COOPER
JEREMY M. BYLUND
SIDLEY AUSTIN LLP
1501 K St., NW
Washington, DC 20005
(202) 736-8000
jgreen@sidley.com

SARAH O. SCHRUP
NORTHWESTERN UNIV.
SUPREME COURT
PRACTICUM
375 East Chicago Ave.
Chicago, IL 60611

Counsel for Amici Curiae

* Counsel of Record

April 9, 2014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES—continued

COURT DOCUMENTS

TABLE OF AUTHORITIES—continued

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*[1]

The National Association of Federal Defenders ("NAFD") was formed in 1995 to enhance the representation provided to indigent criminal defendants under the Criminal Justice Act, 18 U.S.C. § 3006A, and the Sixth Amendment to the Constitution. NAFD is a nationwide, non-profit, volunteer organization. Its membership is comprised of attorneys who work for federal public and community defender organizations authorized under the Criminal Justice Act.

One of the guiding principles of NAFD is to promote the fair administration of justice by appearing as *amicus curiae* in litigation relating to criminal law issues, particularly as those issues affect indigent defendants in federal court. NAFD has appeared as *amicus curiae* in litigation before the Supreme Court and the federal courts of appeals.

NAFD has filed in this case because the indigent criminal defendants served by the organization's members—such as Mr. Wurie in this case—commonly face situations in which they are arrested with cellular telephones on their persons, and an overbroad extension of the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement would open the door to undue

---

[1] Pursuant to Supreme Court Rule 37.6, *amici curiae* state that no counsel for any party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amici* made such a monetary contribution. Both parties have submitted blanket letters of consent to the filing of all *amicus* briefs with the Clerk of the Court pursuant to Rule 37.3.

infringements upon these individuals' right to security in their personal effects.

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense lawyers to ensure justice and due process for persons accused of crime or other misconduct. NACDL was founded in 1958.

NACDL has a nationwide membership of approximately 10,000 and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, active U.S. military defense counsel, law professors and judges. NACDL provides *amicus* assistance on the federal and state level in cases that present issues of importance, such as the one presented here, to criminal defendants, criminal defense lawyers, and the proper and fair administration of criminal justice.

SUMMARY OF ARGUMENT

The First Circuit correctly held that owners of cell phones have a reasonable privacy interest in the data on their phones and that the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement does not categorically authorize warrantless searches of cell phones. The United States' arguments in favor of warrantless searches incident to arrest—evidence destruction and officer safety—revolve around hypothetical actions by third parties. The search-incident-to-arrest exception, however, has always focused solely on the potential actions of the arrestee and responded solely to dangers inherent in each and every arrest.

The exigent circumstances exception to the warrant requirement is a better fit for addressing the United

States' concerns. Applying this doctrine to searches of cell phones will appropriately focus the inquiry on the circumstances of each case, including the speed with which a warrant can be obtained in the subject jurisdiction. Even putting aside this advantage, the bright-line rule proposed by the United States is unworkable because searches of digital information and media cannot be cabined in the manner the United States suggests.

Contrary to the United States' argument, *Smith* v. *Maryland*, 442 U.S. 735 (1979), does not support the warrantless search of cell phone call logs. A call log reveals a broad range of information, including the user's personal routines and the identity of his or her closest intimates. The bare list of dialed numbers at issue in *Smith* is not analogous. Moreover, the mechanical pen register in *Smith* had limited capabilities that ensured there would be no overreach by law enforcement into private information. By contrast, officers ostensibly trying to locate a cell phone's call log could "stumble upon" other information stored on the phone.

The United States is also incorrect in arguing that this Court's decisions in *Maryland* v. *King*, 133 S. Ct. 1958 (2013), and *Florence* v. *Bd. of Chosen Freeholders*, 132 S. Ct. 1510 (2012), support its proposed rule. The decisions in *King* and *Florence* were animated by concerns not present in this case: the need to positively identify arrestees, and the practical necessities of operating safe and secure prisons. Because searching cell phones does not further these goals, *King* and *Florence* do not aid the United States.

ARGUMENT

I. THE FIRST CIRCUIT CORRECTLY HELD THAT THE SEARCH-INCIDENT-TO-ARREST EXCEPTION DOES NOT CATEGORICALLY AUTHORIZE WARRANTLESS CELL PHONE SEARCHES, BUT THAT THE EXIGENT CIRCUMSTANCES EXCEPTION CAN APPLY IN PARTICULAR CASES.

The First Circuit held that "warrantless cell phone data searches are *categorically* unlawful under the search-incident-to-arrest exception, given the government's failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence." Pet. App. 25a (emphasis in original). It further recognized, however, that "other exceptions" to the warrant requirement, particularly the exigent circumstances exception, can justify warrantless cell phone searches "under the right conditions." *Id.* at 28a. This approach is consistent with this Court's precedents and properly recognizes that the exigent circumstances exception provides the appropriate framework for analyzing any exigency-based concerns that arise in this context.

1. In *Chimel* v. *California*, this Court held that when an arrest is made, police can search the arrestee and the area within his immediate control in order to "remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape" and to prevent "concealment or destruction [of evidence]." 395 U.S. 752, 763 (1969). The United States contends that both of these "basic justifications" for the search-incident-to-arrest exception apply in the case of cell phones, U.S. Br. at 42, but it relies on arguments that have no basis in

this Court's decisions. If the Court accepts these arguments here for the first time, it would substantially expand this exception in ways that are untethered to its purposes.

The United States does not claim that cell phone searches are justified under *Chimel* because there is any risk that *arrestees* can use their cell phones to harm police officers or to destroy evidence that is stored on the phones. Nor could it: As Respondent in this case and *amici* in the *Riley* case have amply demonstrated, police officers can fully dissipate such risks by seizing cell phones[2] and removing them from arrestees' control. Instead, the United States claims that risks to police officers and to evidence stored on the phones are posed by the potential *actions of third parties*. See, *e.g.*, U.S. Br. at 37 (contending that an arrestee's "co-conspirators" might attempt to wipe the cell phone data from a remote location); *id.* at 41 (citing risks to officer safety from "confederates or family members" who might head to the scene).

Even assuming that such risks exist,[3] this Court has never held that the potential actions of third parties can serve as a justification for searching an arrestee incident to his arrest. Instead, the search-incident-to-arrest exception is narrowly focused on preventing detrimental actions by the arrestee at the time and place of his arrest. See, *e.g.*, *Chimel*, 395

---

[2] Of course the seizure of the phone would have to be authorized under the search-incident-to-arrest exception, properly considering limiting cases like *Arizona* v. *Gant*, 556 U.S. 332 (2009).

[3] Numerous *amici* in the *Riley* case have demonstrated that police officers have established protocols and techniques for preventing remote wiping of cell phones. *See also* Br. Resp't at 32-34 (showing that the officer safety risk posited by the United States is "highly unlikely").

U.S. at 763 (police can search *an arrestee* and "the area into which an arrestee might reach in order to grab a weapon or evidentiary items . . . ."); *United States* v. *Robinson*, 414 U.S. 218, 234 (1973) (officer safety rationale is based "on the need to *disarm the suspect*" (emphasis added)); *United States* v. *Chadwick*, 433 U.S. 1, 14-15 (1977) (exception is based on the "potential dangers lurking in all custodial arrests" that "*the person arrested* may have a weapon or is about to destroy evidence." (emphasis added)), *abrogated by California* v. *Acevedo*, 500 U.S. 565 (1991); *Gant*, 556 U.S. at 339 (evidence destruction rationale is based on the need to "safeguard[] any evidence of the offense of arrest that *an arrestee* might conceal or destroy" (emphasis added)). As a result, this Court has held that the exception is inapplicable in circumstances where the arrestee can no longer take any actions to harm police officers or destroy evidence. *Chadwick*, 433 U.S. at 15 (search of seized footlocker was "no longer an incident of the arrest" because there was "no longer any danger that the arrestee might gain access" to the footlocker); *Gant*, 556 U.S. at 335, 351 (invalidating search of arrestee's car while he was handcuffed in police vehicle).

Thus, in the guise of asking this Court to hold that searches of cell phones are authorized under the search-incident-to-arrest exception, the United States is really asking this Court to expand the scope of the underlying justifications for the exception. With respect to *Chimel*'s evidence destruction rationale, the United States is asking this Court to hold that a search of an arrestee's cell phone is justified by the mere possibility that third parties will remotely destroy evidence on it. With respect to *Chimel*'s officer safety rationale, the United States does not

contend that a search of an arrestee's cell phone is justified by the possibility that third parties will render the phone dangerous to officers at the scene of the arrest; rather, it contends that officers "can mitigate the risk of danger from sudden arrivals . . . by reviewing the recent calls and text messages of an arrestee's cell phone." U.S. Br. at 41; *id.* at 42 (cell phone "may have information that will warn officers about an imminent dangerous encounter"). In other words, the United States does not contend that the danger to officer safety derives in any way from the cell phone itself. Instead, it contends that warrantless cell phones searches are justified because such searches would be a useful tool for police to combat a danger that they have always had to contend with.

2. This Court should decline to expand the scope of the search-incident-to-arrest exception to encompass the United States' theories. Based as they are on the potential actions of remotely-located confederates, these theories are far removed from the exception's purpose of neutralizing the "potential dangers lurking in *all* custodial arrests," namely, "that the person arrested may seek to use a weapon, or that evidence may be concealed or destroyed." *Chadwick*, 433 U.S. at 14-15 (emphasis added). Because arrestees' cell phones rarely implicate these concerns, the bright-line rule proposed by the United States improperly "diverge[s] from [the] purpose and rationale" of the search-incident-to-arrest exception. *Bailey* v. *United States*, 133 S. Ct. 1031, 1038 (2013). In all cases, "the scope of a search incident to arrest" must be "commensurate with its purposes of protecting arresting officers and safeguarding . . . evidence . . . ." *Gant*, 556 U.S. at 339.

The risk of remote cell phone wiping is hardly one that inherently "lurk[s] in all custodial arrests."

Indeed, the United States has not documented *any* instance of it actually occurring, much less that it is a pervasive risk that justifies blanket authority for police to conduct intrusive cell phone data searches. The absence of real-world examples is not surprising because the risk of remote wiping could only arise if (1) the arrestee has confederates; (2) these confederates are alerted that the arrestee has been taken into custody; and (3) the confederates have the means at hand to wipe the cell phone.[4] These multiple preconditions suggest that the risk of remote wiping arises only in rare cases, not the ordinary course. This conclusion is bolstered by the fact that the "vast majority" of arrests in this country are for alleged misdemeanors, including traffic offenses, for which the arrestee would not have any confederates, much less any reason to arrange for remote wiping in anticipation of a possible arrest. See Br. Pet'r at 2, *Riley* v. *California*, No. 13-132 (S. Ct. Mar. 3, 2014). Even in the case of Mr. Wurie's arrest for alleged drug offenses, there was no evidence that he had any confederates, much less that any third parties attempted to wipe his cell phone.

Because remote wiping is not commonly a danger in making arrests, much less always a danger, there is no justification for granting police blanket authority to conduct warrantless searches of all arrestees' cell phones. Such authority would only create a police

---

[4] *See* Samuel J. H. Beutler, Note, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest*, 15 Vand. J. Ent. & Tech. L. 375, 394 (2013) (explaining that in order for remote wiping to be possible, "(1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to contemporaneously alert the accomplice of the arrest.").

entitlement to indiscriminately rummage through highly private material in the course of the millions of arrests conducted each year.

The United States' officer safety argument is even further removed from the purposes of the search-incident-to-arrest exception, and also foreclosed by this Court's precedent. As noted, the United States does not contend that cell phones themselves pose any sort of danger to arresting officers; instead, its claim is that warrantless cell phone searches would be a useful tool for police because such searches would allow them to identify and anticipate potential threats from confederates who might arrive at the scene. Again, however, the United States has not shown that such threats from confederates arise with any frequency, or that they even arise at all in the ordinary course of arrests. Accordingly, the officer safety concern cannot justify the proposed blanket authorization of warrantless cell phone searches incident to arrest.

Moreover, whatever the usefulness of cell phone searches for monitoring the whereabouts or plans of confederates, this Court consistently has held that "the 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); see also *id.* ("the privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law."); *Coolidge* v. *New Hampshire*, 403 U.S. 443, 481 (1971) (the warrant requirement "is not an inconvenience to be somehow 'weighed' against the claims of police efficiency."); *Bailey*, 133 S. Ct. at 1039-41 (limiting police authority to detain persons incident to execution of search warrant, despite discernible interests in protecting officers and

preventing escape). Thus, no matter how useful or convenient cell phone searches are to police in anticipating the movements of confederates, these law enforcement interests cannot justify dispensing with the warrant requirement in derogation of arrestees' vital Fourth Amendment rights.

For all of these reasons, the First Circuit correctly held that the Fourth Amendment does not permit warrantless cell phone searches to be undertaken as a routine incident of all arrests.

3. This is not to say that police can never conduct warrantless cell phone searches during arrests. As the First Circuit correctly recognized, the exigent circumstances exception is available "under the right conditions," such as "where the phone is believed to contain evidence necessary to locate a kidnapped child or to investigate a bombing plot or incident." Pet. App. 28a-29a. In addition, the exigent circumstances exception is available to address the officer safety and evidence destruction concerns that the United States relies on here—which are essentially exigency-based concerns. This Court consistently has recognized that "law enforcement officers may conduct a search without a warrant to prevent the imminent destruction of evidence," *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1559 (2013) (citing cases), or to "protect or preserve life or avoid serious injury," *Mincey*, 437 U.S. at 392 (quoting *Wayne* v. *United States*, 318 F.2d 205, 212 (D.C. Cir. 1963) (Burger, J., opinion)).

Therefore, in a particular case where police have a reasonable basis to apprehend an imminent risk that third-party confederates will wipe an arrestee's cell phone, or that confederates will arrive at the scene of the arrest and threaten officer safety, the exigent circumstances exception can justify a warrantless

search of the cell phone. Exigency, however, is always a case-specific inquiry based on "the totality of circumstances." *McNeely*, 133 S. Ct. at 1559; *id.* (courts must "evaluate each case of alleged exigency based 'on its own facts and circumstances'" (quoting *Go-Bart Importing Co.* v. *United States*, 282 U.S. 344, 357 (1931))). Although this case-by-case approach provides police with less certainty than a bright-line rule, a bright-line rule is not suitable for the "exigencies" that the United States relies on. These concerns do not arise with any frequency, and their largely hypothetical character renders them insufficient to outweigh the significant privacy interest in the contents of cell phones. See *id.* at 1564 ("While the desire for a bright-line rule is understandable, the Fourth Amendment will not tolerate adoption of an overly broad categorical approach that would dilute the warrant requirement in a context where significant privacy interests are at stake."); see also *Amici* Br. ACLU et al. at 5-9, *Riley* v. *California*, No. 13-132 (S. Ct. Mar. 7, 2014) (highlighting the significant privacy interest owners have in their cell phone data); *Amici* Br. Center for Democracy & Technology and Electronic Frontier Foundation at 5-13, *Riley* v. *California*, No. 13-132 & *United States* v. *Wurie*, No. 13-212 (S. Ct. Mar. 10, 2014) (same); *Amici* Br. Electronic Privacy Information Center et al. at 6-32, *Riley* v. *California*, No. 13-132 (S. Ct. Mar. 10, 2014) (same).

In addition, case-by-case treatment is appropriate in a context, such as this one, where the technology is rapidly changing. In the coming years, remote-wiping techniques may evolve and improve, but so may law enforcement techniques that combat remote wiping. Given this fluid situation, analyzing any issues that arise with respect to remote wiping under a case-by-

case approach ensures that the judiciary does not commit "error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario* v. *Quon*, 560 U.S. 746, 759 (2010).

Moreover, analyzing exigency-based justifications under the exigent circumstances exception allows for consideration of a factor that the United States largely ignores: the speed with which warrants can now be obtained in many jurisdictions. In *McNeely*, this Court recognized that "telecommunications innovations" have significantly "streamline[d] the warrant process" in many jurisdictions. 133 S. Ct. at 1562-63. "Well over a majority of States allow police officers or prosecutors to apply for search warrants remotely through various means, including telephonic or radio communication, electronic communication such as e-mail, and video conferencing." *Id.* at 1562 & n.4 (listing jurisdictions); see also *id.* at 1572-73 (describing expedited procedures used by various states and noting that judges in some jurisdictions "have been known to issue warrants in as little as five minutes," or "in less than 15 minutes.") (Roberts, C.J., concurring in part and dissenting in part). This trend will only continue as "future technological developments" further expedite the warrant process. *Id.* at 1563.

As this Court held in *McNeely*, expedited procedures like these are "relevant to an assessment of exigency." *Id.* Even in those rare situations where police do have reason to fear that confederates might attempt to wipe the arrestee's cell phone, police should be required to obtain a warrant if they can reasonably do so before any likelihood of confederates learning of the arrest and taking action in response arises.

Here, of course, the police had no reason to apprehend that confederates might attempt to wipe Mr. Wurie's cell phone, and the United States did not argue below that the exigent circumstances exception applied. See Pet. App. 1a. This admitted lack of exigency confirms that the search of Mr. Wurie's cell phone was not "commensurate" with any purpose served by the search-incident-to-arrest exception to the warrant requirement.

II. *SMITH* v. *MARYLAND* DOES NOT SUPPORT A RULE ALLOWING CALL LOGS TO BE SEARCHED INCIDENT TO ARREST.

Recognizing the vulnerabilities in its position that police should have blanket authority to conduct warrantless searches of cell phones incident to arrest, the United States alternatively argues that police should be able to conduct searches that are limited in scope. For example, it advocates a bright-line rule allowing police to search all cell phone call logs incident to arrest, U.S. Br. at 54-55, on the view that *Smith* v. *Maryland* establishes that individuals "have no reasonable expectation of privacy" in call logs. U.S. Br. at 54-55. *Smith*, however, hardly stands for that proposition and, indeed, precludes the result that the United States seeks here. In any event, the United States' proposed bright-line rule is unworkable and would invite police to conduct evidentiary fishing expeditions on arrestees' cell phones.

1. The information on cell phone call logs cannot remotely be analogized to the limited information that the police in *Smith* derived from the use of a "pen register," a "mechanical device that record[ed] the numbers dialed" by monitoring the electrical impulses transmitted by a rotary telephone. 442 U.S. at 736 n.1 (quoting *United States* v. *New York Tel.*

Co., 434 U.S. 159, 161 n.1 (1977)). This Court held that because the caller had "voluntarily conveyed" the numbers dialed to the telephone company (by sending electronic impulses over the telephone lines), the caller had no legitimate expectation of privacy in those numbers and thus recording them was not subject to Fourth Amendment protection. *Id.* at 742-45.

Cell phone call logs contain much more information in which owners have a privacy interest than merely numbers dialed. The Court in *Smith* was careful to note that the pen register "does not overhear oral communications and does not indicate whether calls are actually completed." 442 U.S. at 736 n.1 (quoting *New York Tel. Co.*, 434 U.S. at 161 n.1). A cell phone call log, on the other hand, conveys a wealth of information that will only increase as technology advances. Not only do call logs record whether calls were completed, they also record incoming calls, missed calls, the duration of calls, and the time of calls. They disclose the names assigned different contacts by the phone's user. And they provide information about the relative importance of callers to the phone user, based on whether they appear on a speed dial, friend list, or call circle, or just by virtue of the number of communications.

Nicknames and even the spellings of names on the call log can convey private information. In *Riley*, the companion case to *Wurie*, the police noted that the defendant used "CK" in spelling words that usually begin in "k". From that spelling, the police surmised that the defendant was a gang member because "CK" can mean "Crip Killers," which is slang for members of the Bloods gang. Br. Pet'r at 5, *Riley*, No. 13-132. The nicknames that cell phone owners assign to particular contacts can convey a close or intimate

relationship *(e.g.*, "mom," "dad," "boyfriend"), or even medical or mental health information, as by use of a "Dr." prefix or the name of a hotline. Such nicknames can also reveal political affiliations, religious affiliations, and memberships in advocacy groups. Moreover, the frequency of communications, their duration, and the time when they take place can reveal much about the relationship between the phone's user and any given contact. Patterns of communication can also reveal the user's routines and idiosyncrasies, such as his or her ordinary waking hours, work hours, and even diet. The United States' attempt to analogize the exploration of a call log to the use of a pen register to review dialed numbers is thus woefully inapt.

Call logs are also dynamic and continue to record information after the arrest, which makes the search-incident-to-arrest exception an uncomfortable fit. The search-incident-to-arrest exception is justified by officer safety and the need to prevent the destruction of evidence *at the time of arrest*. *Chimel*, 395 U.S. at 763 (police can search an arrestee and "the area into which an arrestee might reach in order to grab a weapon or evidentiary items . . . ."); *Robinson*, 414 U.S. at 234 (officer safety rationale is based "on the need to disarm the suspect"). Allowing police to gather information created *after* the arrest would be an unprecedented expansion of existing doctrine.

The search in this case illustrates that call log searches intrude into the arrestee's privacy far more than the officers intruded in *Smith*. Here, the officers seized Mr. Wurie's phone and, upon opening it, viewed a photograph of a young black woman holding a baby as the phone's wallpaper. Pet. App. 2a-3a. The officers pressed one button on the phone that took them to the call log which indicated incoming calls

from "my house" and pressed one more button to determine the actual number associated with that label. *Id.* Unlike in *Smith*, none of this information was voluntarily conveyed by Mr. Wurie to the telephone company. Created by Mr. Wurie for his own personal use, these digital contents implicate much stronger privacy interests than a bare list of numbers dialed from a rotary phone.

2. Even if the bright-line rule proposed by the United States were legally supportable, it is unworkable and by no means limits the discretion of the police or their access to information on cell phones. While different circuits apply the "plain view" doctrine differently in regard to digital information, there is a considerable amount of information that police can "view" when navigating to a cell phone call log.

In *Smith,* a bright-line rule was possible because the officers only had access to the numbers dialed. *Smith*, 442 U.S. at 737. The very nature of the technology eliminated any concerns about overreach by the police into private information. The Court stressed the limited nature of the intrusion, stating that a pen register does not enable police to "overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 736 n.1 (quoting *New York Tel. Co.*, 434 U.S. at 161 n.1). In the cell phone context, no such technological limitations can cabin police discretion.

The sheer number of different kinds of cell phones, each with their own graphical interfaces, menus, and functionality, makes it much more likely that police will "stumble upon" (either intentionally or inadvertently) additional information while ostensibly trying to navigate to call logs. A "bright-line" rule that depends upon police developing

familiarity with multiple and varied technological devices is no bright-line rule at all.

Compounding the problem, there will undoubtedly be confusion about what constitutes a "search" of a call log, since the United States offers no definition or description. See U.S. Br. at 54 (arguing that police can "search *areas of the phone* for which individuals have no reasonable expectation of privacy—in particular, call logs" (emphasis added)). Can the police click on the number in the call log? Where will clicking on that number take the police? To the contacts list? To a text message and call history screen? To linked pictures to the contact? Allowing police to "search" call logs can easily expand into allowing them to search contact lists, text messages, voice messages, and even photos.

Were police entitled as a categorical matter to access and review call logs, the private information "stumbled upon" might well be admissible under the plain view doctrine. See *Coolidge*, 403 U.S. at 465. The volume of information that could thus be swept in is staggering—and a problem for which there was no analogue in *Smith*.

Case law from the area of computer searches, including searches conducted pursuant to warrants, is replete with examples of law enforcement officers applying the plain view exception to seize evidence of crimes other than the ones they were initially investigating. For example, in *United States* v. *Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999), law enforcement agents were searching a computer for evidence of "unlawfully accessing a government computer," and stumbled upon images of child pornography that the court found to be admissible under the plain view doctrine. *Id.* at 525-29; see also *United States* v. *Stabile*, 633 F.3d 219, 242 (3d Cir. 2011) (declining to

suppress video files with "lurid names" discovered by officer in warranted search for financial information); *United States* v. *Williams*, 592 F.3d 511, 522 (4th Cir. 2010) ("And so, in this case, any child pornography viewed on the computer or electronic media may be seized under the plain-view exception."); *United States* v. *Giberson*, 527 F.3d 882, 884 (9th Cir. 2008) (refusing to suppress evidence of child pornography found on a personal computer during a search for financial information to collect child support); *United States* v. *Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) (rejecting the defendant's claim that emails seized were outside the scope of the warrant because they implicated her in another crime not covered by the search warrant); *United States* v. *Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (applying the plain view doctrine to the discovery of child pornography on a computer in the course of a murder investigation); *State* v. *Mays*, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (holding that an officer's observation of the words "he will die today" on defendant's computer screen while lawfully present in defendant's home fell within the ambit of the plain view doctrine); *Commonwealth* v. *Hinds*, 768 N.E.2d 1067, 1073 (Mass. 2002) (holding that the officer "was not obligated to disregard files listed in plain view on the 'Chuck' directory whose titles suggested contents that were contraband.").

Searches of digital information and media create special problems for the plain view doctrine that are best addressed through requiring police to obtain specific warrants. Courts have struggled with how to cabin searches of digital information even in the warrant context, but have begun to develop useful guidance. See, *e.g.*, *United States* v. *Mann*, 592 F.3d 779, 786 (7th Cir. 2010) ("counsel[ing] officers and

others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."); *United States* v. *Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179-80 (9th Cir. 2010) (Kozinski, C.J., concurring) (providing detailed guidance to judges and prosecutors about search warrant requirements for digital media and the plain view doctrine). The daunting complexities that lie ahead demand close attention from neutral magistrates and ultimately appellate courts, not circumvention by officers "engaged in the often competitive enterprise of ferreting out crime." *Johnson* v. *United States*, 333 U.S. 10, 14 (1948).

3. The United States' reliance on *Smith* is a classic example of a form of reasoning that this Court has cautioned against and rightfully rejected: the wooden application of Fourth Amendment principles and precedents to new technologies. In *United States* v. *Jones*, 132 S. Ct. 945 (2012), for example, this Court rejected the argument that the police could attach a GPS device to a vehicle without a warrant. The United States had argued that the exterior of a car is "thrust into the public eye, and thus to examine it does not constitute a 'search.'" *Id.* at 952 (citation omitted). The Court was not persuaded that a GPS device could be used to continuously monitor a vehicle's location, even though the same information could be obtained through conventional visual monitoring of the vehicle's location by officers. As Justice Sotomayor noted, "[t]he net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may

'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* at 956 (Sotomayor, J., concurring) (quoting *United States* v. *Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

Similarly, in *Kyllo* v. *United States*, this Court rejected "a mechanical interpretation of the Fourth Amendment" because the alternative "would leave the homeowner at the mercy of advancing technology . . . ." 533 U.S. 27, 35 (2001). There, the United States had argued that it could use thermal imaging to detect heat emissions from a house without a warrant. While the dissent argued that any member of the public could detect heat emanations from a home based on observing water evaporation rates or snow melt rates, *id.* at 43 (Stevens, J., dissenting), the majority held that using thermal imaging was a search because the thermal imager allowed the police to "explore details of the home that would previously have been unknowable without physical intrusion," *id.* at 40 (majority opinion).

As *Jones* and *Kyllo* demonstrate, particular care must be taken not to let technological developments rob the Fourth Amendment of relevance. Extending *Smith* to cell phone call logs would do just that. As one judge noted in an analogous context, "the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary . . . I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy." *Klayman* v. *Obama,* No. 13-0881, 2013 WL 6598728, at *19 (D.D.C. Dec. 16, 2013). As in *Klayman*, the pen register example is of little value in

assessing the privacy concerns implicated in searching cell phone call logs.

III. *MARYLAND* v. *KING* AND *FLORENCE* v. *BOARD OF CHOSEN FREEHOLDERS* DO NOT SUPPORT WARRANTLESS CELL PHONE SEARCHES INCIDENT TO ARREST.

The United States relies on *Maryland* v. *King*, and *Florence* v. *Bd. of Chosen Freeholders*,[5] to argue that warrantless cell phone searches are permitted incident to arrest because they "serve the time-sensitive law-enforcement interest in determining or confirming the identity of an arrestee." U.S. Br. 32-33. Relatedly, it relies on these decisions to argue that even if unlimited cell phone searches are unreasonable, "officers should always be permitted to conduct a quick search of a cell phone to confirm a suspect's identity." *Id.* at 52-53. The United States' reliance on these decisions is misguided. It ignores the limited scope of this Court's holdings in those cases and the fact that the Court's actual reasoning compels the rejection of its position in the much different context presented here.

1. The United States principally relies upon *King*, in which this Court upheld Maryland's law authorizing police to collect DNA evidence via cheek swabs from arrestees charged with crimes of violence and other serious crimes. 133 S. Ct. 1958. This Court reasoned that the collection of DNA evidence was justified by law enforcement agencies' "legitimate government interest" in "identify[ing] the persons . . . they must take into custody," *id.* at 1970, and noted that DNA testing provides "an irrefutable

---

[5] *Amici* do not endorse the holdings in *King* or *Florence* and filed *amicus* briefs arguing for different outcomes.

identification," *id.* at 1972. See also *id.* (noting "the unparalleled accuracy DNA provides."). In balancing these law enforcement interests against the "privacy-related" interests of the arrestee, *id.* at 1970, the Court concluded that "the intrusion of a cheek swab to obtain a DNA sample is a minimal one," *id.* at 1977. This is true both because the cheek swab is a "gentle process" that amounts to a "negligible" intrusion, *id.* at 1969, and because the Maryland statute only authorized police to collect and analyze the DNA "for the sole purpose" of ascertaining the arrestee's identity, prohibiting DNA testing that revealed other information, such as the arrestee's "genetic traits" or "private medical information," *id.* at 1979-80.

King does not remotely justify the search of Mr. Wurie's cell phone, much less a categorical rule that cell phones can be searched in order to ascertain arrestees' identities. As an initial matter, the United States' suggestion that the cell phone search at issue enabled police to identify Mr. Wurie does not comport with the facts. See U.S. Br. 32-33. Nothing in the record suggests that there was any uncertainty about Mr. Wurie's identity prior to the search of his cell phone. Police have ample means at their disposal to confirm the identity of arrestees as part of the booking process (*e.g.*, by checking ID's or taking fingerprints), and there is no indication that these means were not conclusive in Mr. Wurie's case. In any event, as the United States acknowledges, the police searched Mr. Wurie's cell phone in order to determine his home phone number and then his place of residence so that they could investigate whether additional contraband would be found at the address, *id.* at 33, not in order to determine his name or identity. In fact, the cell phone search proved

unhelpful in confirming Mr. Wurie's identity: when police cross-referenced the "my house" number with a public online database, the database did not return the name of Mr. Wurie but someone else. Pet. App. 3a (Manny Cristal).

As this case demonstrates, the United States' assertion that "[c]ell phones are particularly useful in identifying an arrestee," U.S. Br. at 32, is anything but self-evident. The United States asserts that a cell phone is "likely" to contain information "indicating" its possessor's real name, "such as text or email messages," *id.*, but this is hardly true in every case. It depends, among other things, on what information an owner chooses to store on the phone, how they label it, what usernames they adopt, and how formally they communicate when using various modes of interaction. In short, the varied contents of cell phones are a far cry from DNA swabs and the "irrefutable identification" they yield. *King*, 133 S. Ct. at 1972.

Indeed, if anything, *King* forecloses the United States' argument. As noted, this Court upheld the DNA swabs in *King* because it found that Maryland's collection of DNA evidence "did not intrude on [arrestees'] privacy in a way that would make his DNA identification unconstitutional." *Id.* at 1979. This was because the procedure was carefully defined and limited by a statute that barred use of samples to index anything apart from "junk" DNA with no known link to genetically identifiable characteristics. *Id.* at 1979-80. By stark contrast, the cell phone searches that the United States advocates here intrude on individuals' fundamental privacy interests. And of course an officer could "stumble upon" all sorts of highly personal information in the course of an ostensible search for "identity"

information. For these reasons, the United States' suggestion that police could conduct "quick" or limited searches to confirm identity "without a close examination of any particularly personal content" is pure fantasy. See U.S. Br. at 52.

In short, *King* provides no authority for the United States' position.

2. *Florence* is even further removed from the issues in this case. In *Florence,* this Court held that correctional officials may subject all detainees who will be admitted to the general prison population to "undergo a close visual inspection while undressed." 132 S. Ct. at 1513. In reaching this conclusion, the Court considered whether the search procedures "struck a reasonable balance between inmate privacy and the needs of the institutions." *Id.* at 1523. It concluded that the searches were justified under this balancing test because "[c]orrectional officials have a significant interest in conducting a thorough search as a standard part of the intake process," *id.* at 1518, in order to discover and "deter the smuggling of weapons, drugs, and other prohibited items inside," *id.* at 1516. Correctional officers also have a legitimate interest in visually inspecting inmates for "certain tattoos and other signs of gang affiliation," as "[t]he identification and isolation of gang members before they are admitted protects everyone in the facility." *Id.* at 1518-19. Given the utility of physical inspections as a means of minimizing potential "danger[s] to everyone in the facility," *id.* at 1522, the government's interest outweighed the privacy interests of persons about to be admitted to a general prison population under conditions affording substantial contact with other detainees, *id.* at 1522-23.

The United States argues that warrantless cell phone searches are permissible because they also can assist police in determining gang affiliation, yet are "comparatively less intrusive" than the visual body searches that this Court upheld in *Florence*. U.S. Br. at 33; *id.* at 52 (noting that this Court "approved exceptionally intrusive searches designed to determine gang affiliation" in *Florence*). This argument is flawed in multiple respects. As an initial matter, the United States' premise that searching personal cell phone data is *per se* less intrusive than visual strip searches is debatable. In any event, the United States ignores that this Court's holding in *Florence* was animated by the unique and serious problems that arise in the context of prison administration—a special area that this Court has identified as meriting a high degree of judicial restraint. See *Florence*, 132 S. Ct. at 1515 ("Maintaining safety and order at these institutions requires the expertise of correctional officials, who must have substantial discretion to devise reasonable solutions to the problems they face."); *Turner* v. *Safley*, 482 U.S. 78, 84-85 (1987) ("Prison administration is, moreover, a task that has been committed to the responsibility of those branches, and separation of powers concerns counsel a policy of judicial restraint."); *Bell* v. *Wolfish*, 441 U.S. 520, 547-48 (1979). *Florence* is simply inapposite, and certainly does not authorize a blanket rule permitting cell phone searches for all arrestees.

CONCLUSION

For these reasons, and those set forth in Respondent's brief, the decision below should be affirmed.

Respectfully submitted,

SARAH S. GANNETT &
DANIEL KAPLAN, CO-CHAIRS
KEITH M. DONOGHUE,
MEMBER
AMICUS COMMITTEE
NAT'L ASS'N OF FEDERAL
DEFENDERS
601 Walnut St., Ste. 540W
Philadelphia, PA 19106

MASON C. CLUTTER
NAT'L ASS'N OF CRIMINAL
DEFENSE LAWYERS
1660 L St., NW
Washington, DC 20036

JEFFREY T. GREEN*
JACQUELINE G. COOPER
JEREMY M. BYLUND
SIDLEY AUSTIN LLP
1501 K St., NW
Washington, DC 20005
(202) 736-8000
jgreen@sidley.com

SARAH O. SCHRUP
NORTHWESTERN UNIV.
SUPREME COURT
PRACTICUM
375 East Chicago Ave.
Chicago, IL 60611

Counsel for Amici Curiae

* Counsel of Record

April 9, 2014