**Nos. 13-132 & 13-212**

# In the Supreme Court of the United States

DAVID LEON RILEY,

*Petitioner,*

v.

STATE OF CALIFORNIA,

*Respondent.*

UNITED STATES OF AMERICA,

*Petitioner,*

v.

BRIMA WURIE

*Respondent.*

**On Writs of Certiorari to the California Court of Appeal, Fourth District and the United States Court of Appeals for the First Circuit**

## BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AND ELECTRONIC FRONTIER FOUNDATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER IN NO. 13-132 AND RESPONDENT IN NO. 13-212


EUGENE R. FIDELL
*Yale Law School*
*Supreme Court Clinic*
*127 Wall St.*
*New Haven, CT 06511*
*(203) 432-4992*

ANDREW J. PINCUS
*Counsel of Record*
CHARLES A. ROTHFELD
MICHAEL B. KIMBERLY
PAUL W. HUGHES
*Mayer Brown LLP*
*1999 K Street NW*
*Washington, DC 20006*
*(202) 263-3000*
*apincus@mayerbrown.com*

*Counsel for* Amici Curiae

## QUESTION PRESENTED

*Amici Curiae* will address the following question:

Whether the search-incident-to-arrest doctrine authorizes the government to search—without a warrant and without probable cause—the digitally-stored information contained in a portable electronic device found on the person or within the control of an individual at the time of his or her arrest.

## TABLE OF CONTENTS

**TABLE OF CONTENTS—continued**

## TABLE OF AUTHORITIES

**Cases**

## TABLE OF AUTHORITIES—continued



### Other Authorities

**TABLE OF AUTHORITIES—continued**

**TABLE OF AUTHORITIES—continued**

**TABLE OF AUTHORITIES—continued**

**TABLE OF AUTHORITIES—continued**

## INTEREST OF THE *AMICI CURIAE*

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing civil liberties issues raised by emerging technologies.

CDT and EFF have participated as *amici* in cases before this Court involving the application of the Fourth Amendment to new technologies, including *City of Ontario* v. *Quon*, 560 U.S. 746 (2010), and *United States* v. *Jones*, 132 S. Ct. 945 (2012).[1]

## SUMMARY OF ARGUMENT

Modern cell phones and other portable electronic devices contain very large amounts of sensitive, personal information—including an archive of communications with family and close friends, the equiva-

---

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici* and their counsel made a monetary contribution to its preparation or submission. The parties' letters consenting to the filing of this brief have been filed with the Clerk's office.

lent of bookshelves worth of photo albums, and substantial personal medical and financial information.

Prior to the advent of digital technology, this information would have been stored in the drawers and file cabinets of people's homes. Law enforcement officers would have been required to obtain a warrant in order to search such materials.

The question before the Court is how the Fourth Amendment applies in light of this significant advance in technology—in particular, whether the search-incident-to-arrest exception authorizes warrantless searches of all of the information stored digitally on a portable electronic device found on an arrested individual's person.

Permitting warrantless searches of this large amount of information is inconsistent with the Fourth Amendment for three reasons.

*First*, the search-incident-to-arrest exception was recognized in the earliest days of our Nation, when information could be transported only if it was written on paper. That reality imposed a significant inherent limitation on the scope of the exception: because the amount of information an individual could carry was restricted by the weight and bulk of paper, the exception's intrusion on sensitive personal information would be circumscribed.

Technology now makes it possible for individuals to carry huge quantities of information with them every day. Permitting warrantless searches of digitally-stored information will allow police to rummage through vast quantities of individuals' personal information—precisely what the Framers of the Fourth Amendment sought to prevent.

*Second*, neither of the justifications for the exception support a search of the data stored on an electronic device. An inspection of the device is sufficient to establish that it poses no threat to police officers. And once the police officer has seized the device there is no risk that the arrestee himself will be able to access the device and destroy evidence. If the risk of destruction of evidence is present in a particular case—because the officers reasonably believe that the particular device's digitally-stored information will be deleted by the actions of a third party or other means that they cannot prevent using reasonably-available countermeasures—the well-established exigent circumstances exception will allow officers to act to preserve the information (but not search it) without obtaining a warrant.

*Third*, a bright-line rule requiring police officers to obtain a warrant before searching digitally-stored information is clear and therefore easily administrable. Standards under which the need for a warrant would turn on the relative sophistication of the particular portable electronic device would be impossible for officers to apply—they could not possibly keep track of the various relative capabilities of the myriad different types and models of these devices. Similarly, a rule that allows officers to search some categories of information but not others makes no sense because these devices increasingly are designed to integrate the different categories of information stored on the device and to seamlessly access remotely-stored data in ways that make it indistinguishable form the data stored on the device.

Finally, the warrant requirement is not burdensome. Once police have seized the device, it will not be difficult to present the warrant request to a judi-

cial officer and, if probable cause is shown, obtain the authorization that the Fourth Amendment requires.

## ARGUMENT

### THE SEARCH INCIDENT TO ARREST DOCTRINE DOES NOT AUTHORIZE WARRANTLESS SEARCHES OF INFORMATION STORED ON AN ELECTRONIC DEVICE.

This Court has recognized repeatedly that the Fourth Amendment's protections against government intrusions must be construed in light of the nature and effects of advances in technology. *United States* v. *Jones*, 132 S. Ct. 945 (2012); *City of Ontario* v. *Quon*, 560 U.S. 746 (2010); *Kyllo* v. *United States*, 533 U.S. 27 (2001).

When new technologies would allow the government to access previously unavailable information, the Court has taken those developments into account in delineating the Fourth Amendment's protections. See, *e.g.*, *Jones*, *supra* (GPS tracking device); *Kyllo*, *supra* (thermal imaging device); *Katz* v. *United States*, 389 U.S. 347 (1967) (wiretap of payphone); cf. *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562-1563 (2013) (acknowledging that "technological developments that enable police officers to secure warrants more quickly * * * are relevant to an assessment of exigency").

That same need to consider the impact of advances in technology is presented in these cases as a result of innovations permitting digital storage of large amounts of information on increasingly ubiquitous portable electronic devices. Although the searches here involved information stored on cell phones, the federal government recognized below that its legal theory is not limited to those particular

devices and would permit the search of all digitally-stored data on "any electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device such as an iPad." 13-212 Pet. App. 15a.

### A. Modern Cell Phones And Other Portable Electronic Devices Contain Enormous Amounts Of Sensitive Personal Information That Individuals Formerly Kept In Their Homes.

Advances in digital technology permit the storage on portable electronic devices of huge amounts of personal information—including communications with family and friends, diaries, pictures, and financial and health records—that individuals typically kept in their homes before the digital era. This information is generated in substantial part as a result of innovations that permit the use of these portable devices to send and receive email and text messages, and to perform a myriad of other functions.

The two cases before the Court involve cell phones, but many different types of portable electronic devices have the information-storage and other characteristics of cell phones.[2] For example, tablet computers and laptop computers have extensive storage, computing, and communication features.[3]

---

[2] All of these devices, like cell phones, store data electronically in a series of *1*'s and *0*'s. Conner Technical Services, http://perma.cc/QN3L-XT8R) ("The only [numbering system] * * * that an electronic device uses is binary * * * .").

[3] Christopher Barnatt, *A Guide to Computing: Mobile Computing* (Nov. 2, 2013), http://perma.cc/TWU9-VVTZ (explaining that modern laptops have the same functionality as desktop computers). Modern tablets allow a user to "browse the inter-

Digital cameras have substantial storage capabilities—for both still pictures and video, including sound.[4] And "thumb drives," small devices no larger than a thumb, can also store huge quantities of data.[5]

Thus, although we focus below on the capabilities of modern cell phones, those capabilities are shared by a significant number of other portable electronic devices that individuals routinely carry on their persons. And the variety of such devices is growing significantly as innovators find new ways to use electronic communications, storage, and computing technologies.

Modern cell phones[6] are ubiquitous: 91% of American adults own one.[7] These devices have dra-

---

net, create and share presentations, video[] conference with clients, stay connected with corporate email, download books, games and videos, watch movies, share photos and much more * * * ." *Tablet: What is it? Which Tablet is Right for Me?*, Staples Advantage, http://perma.cc/AAG7-H566.

[4] The basic storage medium for images and video on a digital camera—flash memory—sells for $12 at 16 GB, which can hold 8,000 images or one hour of high-resolution video with sound. See *SanDisk Ultra 16 GB*, Amazon.com, http://perma.cc/ALS6-SU9F. Recently released memory cards for cameras already store up to four times more data than today's cell phones. See Consumer Electronics, 2013 WLNR 27310700 (Oct. 28, 2013) (noting that SanDisk released a 256 gigabyte memory card to keep up with developments in photography and videography).

[5] Even a small and simple thumb drive, which holds 2 GB of data and sells for less than four dollars at Walmart, see http://perma.cc/YZD5-MCFX, can hold up to one thousand photographs, *USB Flash Drives: How Much Storage Space is Enough?*, eBay, http://perma.cc/D4MQ-HV8X.

[6] Modern cell phones are sometimes described using two general, and overlapping, terms—"feature phone" and "smartphone." A smartphone is "[a] cellular telephone with built-in

matically expanded the amount and types of information that Americans carry every day.

The amounts of information that these devices can contain are staggering. For example:

- The Apple iPhone 5 is the largest-selling smartphone;[8] the version with the smallest storage capability (16 gigabytes ("GB")) can store 800 million words of text[9]—well over a

---

applications and Internet access. In addition to digital voice service, modern smartphones provide text messaging, e-mail, Web browsing, still and video cameras, MP3 player and video playback and calling." *Definition of: Smartphone*, PC Magazine Encyclopedia, http://perma.cc/647Z-MGRW. Feature phones usually contain "a fixed set of functions beyond voice calling and text messaging, but [are] not as extensive as a smartphone." *Definition of: feature phone*, PC Magazine Encyclopedia, http://perma.cc/6RHP-DKRG. Thus, both types of phones store data digitally, and both provide text messaging and some common additional features, with smartphones providing a wider array of such features. We use "modern cell phones" to refer to both categories, unless specifically noted otherwise.

[7] Pew Research Center, *Cell phone ownership hits 91% of adults* (June 6, 2013), http://perma.cc/ALM7-QZBJ ("[T]he cell phone is the most quickly adopted consumer technology in the history of the world.").

[8] See Shane Cole, *Apple's iPhone 5s remains 'by far the top selling smartphone*,' Apple Insider (Dec. 12, 2013, 8:06 AM), http://perma.cc/PP3W-XQZV.

[9] *The Amazing History of Information Storage: How Small Has Become Beautiful*, Statistical Trends & Numbers (Aug. 12, 2012), http://perma.cc/9PFX-DPEE (noting that the complete 2010 Encyclopedia Britannica, which contains 32 volumes, weighs 129 pounds in physical form, and contains 50 million words, could fit in a single gigabyte of data).

football field's length of books[10] or, to use another measure, sixteen flat-bed truckloads of paper.[11]

- The same phone can contain over 8,000 digital pictures,[12] over 260,000 private voicemails,[13] or hundreds of home videos.[14]
- Other versions of the iPhone, with 32 GB or 64 GB of storage capacity, would be able to store twice or four times those amounts. Some manufacturers have produced phones with 128 GB memory—and therefore the ability to store *eight times* the amount of information contained on a 16 GB phone.[15]

These examples describe the storage capacity of modern cell phones in terms of "books," "photo-

---

[10] An American football field, including end zones, is 120 yards long. Since "1 Gigabyte could hold the contents of about 10 yards of books on a shelf," 16 GB would correspond to about 160 yards of books. *Megabytes, Gigabytes, Terabytes ... What Are They?*, What's a Byte, http://perma.cc/8AAW-MVZQ.

[11] *How much data is there on a hard drive?*, Ctr. for Computer Forensics, http://perma.cc/T6CL-JTHG.

[12] *Number of pictures that can be stored on a memory device*, SanDisk, http://perma.cc/J7JW-7AC7.

[13] Assuming each voicemail lasts thirty seconds and is recorded at a bitrate of 16 kbps, a 16 GB device could hold over 266,666 voicemails.

[14] Assuming each home video is thirty seconds long, recorded at standard definition, 16 GB could store 480 such videos. See Derek Fung, *What Storage Should I Get in My Camcorder?*, CNET Australia (Sept. 23, 2009), http://perma.cc/QHX9-KNQ6.

[15] See Richard Lai, *World's first 128GB phone now available from Meizu, but only works in China*, Engadget (Nov. 18, 2013), http://perma.cc/SN77-V24S.

graphs," "videos," and "voicemails" for ease of explanation, but the information is stored on these devices in many different forms—including text messages, e-mails, Internet browsing records, documents, diary entries, "to do" lists, and sound recordings, as well as books, photographs and videos. And they typically include individuals' most personal information in each of these categories.

*First*, messages to or from family and close friends are often memorialized as emails, text messages, or voicemail messages. The user's own personal thoughts are contained in an electronic diary or notes or other documents. Photographs and video recordings capture an individual's most personal moments.

These devices' extensive storage capacity means that they do not contain messages, personal thoughts, or photographs and videos from only the last several days, or only the last several weeks. Rather, they can and frequently do retain this information from prior months or even years.

Before the development of portable devices with extensive digital storage capability, of course, it would have been impossible for anyone routinely to carry on his or her person more than a few days' worth of these materials. The vast majority of the information that today is stored digitally on these devices would have been stored in the individual's home or office.

*Second*, electronic appointment calendars on cell phones store sensitive information about a user's daily activities—including appointments with doctors of all types, religious advisors, psychiatrists, therapists, drug or alcohol-treatment groups, grief counselors,

political groups, marital counselors, and fertility consultants, among many others. And, because these calendars preserve past appointments, they provide a detailed, multi-year record of the user's activities—something that individuals would not ordinarily carry every day before the invention of these devices.

*Third*, modern cell phones also list the telephone calls made from or received by the phone, but typically integrate that data with other information stored on the phone. That integration function often provides the name, address, and other information regarding the individual associated with the particular phone number, such as his or her relationship to the cell phone's owner.[16]

*Fourth*, the ability of modern cell phones to function as computers—with an incredibly varied capabilities provided by software programs called "applications" or "apps"—means that these devices often perform functions that result in the storage on the device of additional types of information.

Thus, Electronic Health Record (EHR) "apps" are widely available for smartphones; they are used by both medical professionals and patients to keep track of private medical information in electronic form.[17] Other medical information apps include diabetes

---

[16] Google's popular Gmail email service, for instance, is linked to its "Contacts" address book feature, which is also linked to its Google+ social network feature. See Alexei Oreskovic, *Google's new Gmail feature linking social network contacts raises privacy concerns*, Financial Post (Jan. 10, 2014, 11:56 AM), http://perma.cc/QL5U-MVM3.

[17] See, *e.g.*, *Compare iPad Electronic Medical Records Software*, Software Advice, http://perma.cc/K3FH-DJLY.

tracking apps,[18] apps to help smokers quit,[19] and Alzheimer's disease apps.[20] These apps result in the storage on the cell phone of users' most intimate medical information.

Personal finance apps cause the storage on the cell phone of similarly sensitive financial information, because they link to bank accounts, keep track of investments, and catalog assets. These apps "extract real-time data from your service providers—including banks, investment houses, lenders, and credit card companies," replacing "the pre-PC days when tracking your expenses involved saving receipts, writing down transactions, [and] opening paper bills."[21]

Again, prior to the development of these storage, communication, and computing technologies, individuals would not carry this information with them every day. Sensitive financial and medical information would be kept at home or in the office, with selected physical documents placed in a purse or briefcase only if needed for a particular purpose on a particular day.

*Fifth*, many modern cell phones routinely use Global-Positioning-System ("GPS") data to determine

---

[18] See, *e.g.*, *The 13 Best Diabetes iPhone & Android Apps of 2013*, Healthline (Aug. 8, 2013), http://perma.cc/UPY9-EGTS.

[19] See, *e.g.*, *Smokefree Apps*, Smokefree.gov, http://perma.cc/4QBP-8DZR.

[20] See, *e.g.*, Rob LeFebvre, *New App For People With Alzheimer's Launches Today, Free For Limited Time*, Cult of Mac (Aug. 19, 2013, 11:00 AM), http://perma.cc/QS9Y-TQT4.

[21] Jill Duffy, *Best Mobile Finance Apps*, PC Magazine (Oct. 8, 2013), http://perma.cc/QS9Y-TQT4.

the phone's location whenever the phone is turned on—because location information is used in many apps.[22] That GPS data is archived, providing a record of the user's movements any time the phone is turned on.[23] The highly personal nature of this information was recognized by the Court in *United States* v. *Jones*. See 132 S. Ct. at 963-964 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment); *id*. at 955-956 (Sotomayor, J., concurring).

Moreover, technology is continuing to evolve. New devices such as smart watches and Google Glass will increase the types and amounts of electronically-stored personal information that individuals carry with them each day. Thus, "[a] smartwatch packed with sensors designed to provide body monitoring information could enable many fascinating new data-driven applications, from fitness tracking to mood-linked music commanded by your heartbeat. * * * Apple holds patents for sensory information collection, including blood-pressure monitoring."[24]

---

[22] For example, the popular application Foursquare "use[s] the location information from your mobile device to tailor the Foursquare experience to your current location." *Does Foursquare track my location?*, Foursquare Help Center, http://perma.cc/-U63C-CHNM.

[23] See Charles Arthur, *iPhone keeps record of everywhere you go*, The Guardian (Apr. 20, 2011), http://perma.cc/S6LC-4UN8. Moreover, cell phone companies also store location data for extended periods, often years. *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, http://perma.cc/J2R7-9N6B.

[24] Samuel Gibbs, *Apple's iWatch*: *What Features Are on Our Wishlist?*, The Guardian (Feb. 4, 2014, 5:14 PM), http://-perma.cc/A4V6-D6WN.

Similarly, "Google Glass, the Internet-connected eyewear" could "lead to a world in which people wear or even ingest computers" that monitor and store a wide variety of individuals' personal medical information.[25]

### B. The Search-Incident-To-Arrest Exception Does Not Extend To Searches Of Electronically-Stored Data.

The search-incident-to-arrest doctrine is an exception to the Fourth Amendment's generally-applicable requirements of a warrant and probable cause. Given the significant privacy interests at stake, law enforcement officers must obtain a warrant to search digitally-stored data on cell phones and other portable electronic devices.

#### *1. The Balance Of Interests Underlying The Exception Does Not Support Blanket Authorization Of Warrantless Searches Of Digitally-Stored Personal Information.*

"In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *Jones*, 132 S. Ct. at 963 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment). That is particularly true of the search-incident-to-arrest exception.

The exception has deep roots. A century ago this Court stated that it was "always recognized under

---

[25] Claire Cain Miller, *Google Glass to Be Covered by Vision Care Insurer VSP*, N.Y. Times (Jan. 28, 2014), http://perma.cc/H6AR-96YG. Indeed, digital devices such as pacemakers already installed in the human body can store data such as one's heart rate and breathing rate. *What Is a Pacemaker?*, National Heart, Lung, and Blood Inst., http://perma.cc/4UCA-XEQB.

English and American law." *Weeks* v. *United States*, 232 U.S. 383, 392 (1914); see also *Virginia* v. *Moore*, 553 U.S. 164, 170 (2008) ("[S]earches incident to warrantless arrests * * * were * * * taken for granted at the founding.") (quotation marks omitted).

At that time, the amount of personal information that an arrestee could carry on his person or have within his control was quite limited. Information could be carried only in physical form—as papers (and later as photographs).

Because of that physical limitation, individuals typically carried with them only the documents needed for that day's activities, plus whatever else might be useful provided that it would fit in a wallet, address book, or briefcase or purse. Individuals did not (and could not) routinely carry large amounts of personal correspondence, photograph albums (or painted family portraits), financial records, or other private information. That information was stored in the individual's home or office.

From the time of its creation until very recently, therefore, the exception had a built-in limitation: the amount of paper that an individual could carry on his or her person or have within his or her reach at the time of arrest. See *Chimel* v. *California*, 395 U.S. 752, 763 (1969) (holding that a search incident to arrest encompasses the arrestee's person and space "within his immediate control").

That physical reality, and the exception's resulting inherent limitation, explains why the search-incident-to-arrest exception was fully compatible with the Founders' determination to prohibit the general warrants and writs of assistance authorizing indiscriminate searches. See, *e.g.*, *Chimel*, 395 U.S.

at 761; *Weeks*, 232 U.S. at 390 (discussing the Fourth Amendment's origin). Because individuals did not routinely carry all, most, or even many of their private papers with them each day, there was no danger that the exception would be abused to permit rummaging through an individual's most private papers—those papers were safely at home, where, even after the homeowner's arrest, a warrant would be required to search them.

Modern technology has fundamentally changed the amount and nature of the personal information that an individual typically carries and has within his or her reach.

To take one example, the Library of Congress's collection of James Madison's papers consists of approximately 72,000 pages of documents.[26] Madison did not and could not carry those documents on his person—they would have weighed at least 675 pounds.[27] They were kept in his home and in the homes of his correspondents.

Today, however, a cell phone can contain more than 100 times the number of pages in the entire Madison collection.[28] Digital data storage makes it possible for Americans to carry with them every day vast quantities of sensitive information that previously was kept within their homes. See pages 5-13,

---

[26] See *James Madison Papers*, Library of Congress, http://perma.cc/LPS5-45NG.

[27] *How Much Does a Ream of Paper Weigh?*, Ask.com, http://perma.cc/7WQ5-2HCB (noting that a ream of paper weighs approximately 4.7 pounds).

[28] Assuming 400 words per page, a 16 GB iPhone can hold 800 million words, or 2 million pages. See note 9, *supra*. A 64 GB iPhone can hold 8 million pages.

*supra*. Moreover, the breadth of that information would likely reveal an individual's medical history, religious beliefs, political affiliations, network of friends, colleagues, intimate associates, and acquaintances.

Allowing law enforcement officers to conduct warrantless searches of this electronically-stored information therefore cannot be justified based on precedents that necessarily rest on the much narrower intrusion on privacy interests that could possibly have resulted from searches-incident-to-arrest of physical, rather than digital, materials. Given the dramatically broader intrusion that would result from a blanket authorization of warrantless searches of all digitally-stored information—akin to the significant intrusion that the Fourth Amendment was intended to prevent—those precedents cannot support extension of the exception into this new context.

Indeed, the United States' mechanical invocation of precedent divorced from context here closely resembles the argument that the government advanced—and a majority of the Court rejected—in *United States* v. *Jones*. There, the government argued that precedents finding no reasonable expectation of privacy in an individual's movements on public streets, because of police officers' ability to observe those movements, meant that GPS tracking did not constitute a Fourth Amendment search.

A majority of the Court rejected that argument. 132 S. Ct. at 964 (Alito, J., with whom Ginsburg, Breyer, and Kagan, JJ., joined, concurring in the judgment) (finding a Fourth Amendment search because "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 956 (Sotomayor, J., concurring) (recognizing that the "attributes of GPS monitoring" must be taken "into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements"); see also *Kyllo*, 533 U.S. at 34 (refusing to "permit police technology to erode the privacy guaranteed by the Fourth Amendment").

Fourth Amendment search-incident-to-arrest decisions that rest upon completely inapplicable assumptions should be held inapplicable here for the same reason. New technology permits a very substantial intrusion on core Fourth Amendment interests that was not anticipated, and could not have been anticipated, when the search-incident-to-arrest exception was recognized.

The federal government argues that the doctrine is nonetheless applicable, repeatedly referencing "the reduced expectations of privacy triggered by the fact of arrest." No. 13-212 U.S. Br. 19. This Court, however, has rejected the notion that "any search is acceptable solely because a person is in custody. Some searches, such as invasive surgery, or a search of the arrestee's home, involve either greater intrusions or higher expectations of privacy." *Maryland* v. *King*, 133 S. Ct. 1958, 1979 (2013) (internal citations omitted). If "the privacy-related concerns are weighty enough * * * the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Ibid.*

Here, the intrusion on privacy interests from routine searches of digitally-stored information would be very substantial, because of the large amounts of personal information stored on portable

electronic devices. And, as we next discuss, neither the law enforcement interests underlying the search-incident-to-arrest exception nor other law enforcement interests come close to justifying warrantless searches of this information.

*2. The Justifications For The Search-Incident-To-Arrest Exception Do Not Apply To Electronically-Stored Data.*

In *Chimel* v. *California*, 395 U.S. 752 (1969), the Court explained the "analysis [that] underlies the 'search incident to arrest' principle, and marks its proper extent." *Id*. at 762; accord *Arizona* v. *Gant*, 556 U.S. 332, 343 (2009) (refusing to "untether" the exception from *Chimel*'s justifications).

The federal government argues that *Chimel* is irrelevant, because the Court's decision in *United States* v. *Robinson*, 414 U.S. 218 (1973), recognizes plenary authority to search any object found on the arrestee's person. See No. 13-212 U.S. Br. 17-28. That contention is wrong for two reasons.

To begin with, it ignores the fundamentally different question presented by application of the search-incident-to-arrest exception to digitally-stored information. For the reasons discussed above, any such blanket rule should not be extended to this extremely different context.

But the government's argument is also wrong on its own terms. *Robinson*'s focus was the lower court's narrow view of a police officer's authority to search an arrestee—the court of appeals had held that the officer "may not ordinarily proceed to fully search the prisoner" but could only "conduct a limited frisk of the outer clothing and remove such weapons that he may, as a result of that limited frisk, reasonably be-

lieve and ascertain that the suspect has in his possession." 414 U.S. at 227.

This Court squarely rejected that conclusion, holding that "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." *Id.* at 235. That holding says nothing about searches of objects found on the arrestee's person.

Only one sentence of the *Robinson* opinion addressed that question. The Court stated: "Having in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them * * *." *Id.* at 236.

The Court did not explain why the officer was "entitled to inspect" the package. Most likely, it was because, as the government itself argued in *Robinson*, that further search was justified to determine that the package did not contain a weapon. See No.13-132 Pet. Br. 18 (discussing government's argument).

But the Court's unexplained conclusory statement certainly provides no basis for transforming *Robinson*'s holding—that officers may conduct a full search of the arrestee's person—into authority for officers to conduct a full search of everything found on his person, even if *Chimel*'s justifications do not apply.

That is especially true because, as the government acknowledges, the officers' ability to search without a warrant objects not found on the arrestee's person does turn on whether those justifications are

present. No. 13-212 U.S. Br. 21-23. In the government's view, therefore, it may download the full contents of a cell phone without a warrant if the phone is in the arrestee's pocket, but it may not do so if the phone is on the seat next to him. Given the very substantial amount of personal information involved, it is nonsensical for the warrant requirement to turn on such a distinction.

The question in both situations is whether the *Chimel* justifications for the search-incident-to-arrest exception apply. And neither of the two rationales identified in *Chimel* permits searches of the electronically-stored contents of a cell phone.

*First*, the exception rests on the determination that "it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape." *Chimel*, 395 U.S. at 763. Removal of the mobile phone from the arrestee's possession and examination by the officers to ensure that it is not a disguised weapon (and that it cannot be used by the arrestee to summon his confederates) are all that is necessary to fulfill that purpose.

*Second*, "it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." *Id.* at 763. The sole concern is the risk of concealment or destruction of evidence *by the arrestee*. *Chimel* explained that the justification extends to a search of "the area 'within his immediate control'—construing that phrase to mean the area from within which [the arrestee] might gain possession of * * * destructible evidence." *Ibid.*

That is why "the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant's arrest *only when* the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." *Gant*, 556 U.S. at 343 (emphasis added); see also *United States* v. *Chadwick*, 433 U.S. 1, 15 (1977) (stating that once the officers had "exclusive control," "there [was] no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence"), abrogated on other grounds by *California* v. *Acevedo*, 500 U.S. 565 (1991).

Once law enforcement officers have arrested an individual and seized his or her cell phone, there is no possibility that the arrestee himself will be able to act to delete the information it contains. Accordingly, the "preservation of evidence" prong of *Chimel* is also inapplicable.

The government argues (No. 13-212 U.S. Br. 34-40) for a much more expansive interpretation of this aspect of *Chimel*, asserting that the mere possibility that evidence might be destroyed by the actions of a third party or through a device previously installed by the arrestee is sufficient to trigger the exception. It points to the availability of cell phone "wiping" technology that may be activated by a signal sent by a third party or by the arrestee's failure to enter a code at specified time intervals. *Id.* at 37-39.

That argument is flawed on multiple grounds. To begin with, the consequences of expanding *Chimel*'s rationale to encompass the risk that the arrestee may have taken prior action that would result in destruction of evidence or that third parties would act to destroy evidence would dramatically broaden the government's authority. It always is possible that an

arrestee also could have instructed his accomplices to destroy evidence if he did not return to his home by a specified time. Does that mere possibility mean that officers may undertake a warrantless search of every arrestee's home? Does the possibility that a closed container might be booby-trapped to destroy any incriminating materials that it contained mean that police officers may override *Chadwick*'s limitation on the exception?

No decision of this Court endorses such a broad approach. As we have discussed, this Court has made clear that a search is not permissible once the arrestee cannot gain possession of the potential evidence—which will always be the case after the phone has been seized by the officers.[29]

Moreover, there is no support for the government's implicit contention that the use of wiping technologies is widespread and cannot be counteracted, or that the use of passwords—common in a variety of other contexts—somehow justifies expanding the exception. See No. 13-132 Pet. Br. 22-24.

Finally, "a broad reading of [*Chimel*] is also unnecessary to protect law enforcement * * * evidentiary interests." *Gant*, 556 U.S. at 346. As was the case with respect to the overbroad construction of the search-incident-to-arrest exception rejected in *Gant*, "[o]ther established exceptions to the warrant requirement authorize [searches] under additional cir-

---

[29] As we discuss below (at page 28), the government's argument is really a claim for an across-the-board determination that searches of digitally-stored information are always justified by exigent circumstances–something that is not permissible under exigent search principles.

cumstances when safety or evidentiary concerns demand." *Ibid.*

A warrant is not required if "'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." *Brigham City* v. *Stuart*, 547 U.S. 398, 403 (2006) (quoting *Mincey* v. *Arizona*, 437 U.S. 385, 393-394 (1978)). One such circumstance occurs when an officer is faced with "the imminent destruction of evidence." *McNeely*, 133 S. Ct. at 1559; see, *e.g.*, *Illinois* v. *McArthur*, 531 U.S. 326, 331 (2001) (concluding that a warrantless seizure of a person to prevent him from returning to his trailer to destroy hidden contraband was reasonable "[i]n the circumstances of the case before us" due to exigency); *Cupp* v. *Murphy*, 412 U.S. 291, 296 (1973) (holding that a limited warrantless search of a suspect's fingernails to preserve evidence that the suspect was trying to rub off was justified "[o]n the facts of this case").

"'[T]he fact-specific nature of the reasonableness inquiry,' demands that we evaluate each case of alleged exigency based 'on its own facts and circumstances.'" *McNeely*, 133 S. Ct. at 1559 (internal citations omitted). If officers have specific knowledge that the contents of a particular phone may be lost due to a wiping program or some other technology, and they believe that the contents cannot be preserved while they seek a warrant, they may be able to satisfy the exigent circumstances test.

Importantly, that exigency could justify only the downloading of the digitally-stored information for purposes of preservation, not a search of that information (police patrol cars increasingly are outfitted with the technology to perform such downloads at

the time and place of arrest). A warrant still would be needed to search the information.

Law enforcement officers also do not need a warrant to observe items within their "plain view." "[A] truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion." *Arizona* v. *Hicks*, 480 U.S. 321, 328 (1987).

If an incoming call, text message, or other information appears on the face of the phone, an officer may view that information without a warrant. That aspect of the officers' actions in *Wurie* was permissible. 13-212 Pet. App. 2a ("[O]ne of Wurie's cell phones * * * was repeatedly receiving calls from a number identified as 'my house' on the external caller ID screen on the front of the phone[ and] [t]he officers were able to see the caller ID screen, and the 'my house' label, in plain view.").

But by going on to "open[] the phone" and press a button to "access the phone's call log," review the call log, and "press[] one more button" to search for the suspect's contact information (Pet. App. 3a), the officers moved beyond merely observing information in plain view. The plain view doctrine accordingly cannot justify the federal government's use of the information gained from the officer's manipulation of the phone.[30]

---

[30] Police officers also may conduct "inventory searches"—"[a]t the stationhouse, it is entirely proper for police to remove and list or inventory property found on the person or in the possession of an arrested person who is to be jailed." *Illinois* v. *Lafayette*, 462 U.S. 640, 646 (1983). An officer therefore could ob-

* * * * *

This Court in *Gant* rejected an expansive interpretation of the search-incident-to-arrest exception in part because it "seriously undervalue[d] the privacy interests at stake." 556 U.S. at 344-345. Law enforcement officers would have been able "to search not just the passenger compartment [of the car] but every purse, briefcase, or other container within that space." *Id*. at 345.

Permitting the police to conduct such a search in connection with every single traffic offense arrest would have "create[d] a serious and recurring threat to the privacy of countless individuals. Indeed, the character of the threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." *Ibid*.

---

serve the exterior of an arrestee's cell phone and include it on the list of the arrestee's property.

"[A]n inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence." *Florida* v. *Wells*, 495 U.S. 1, 4 (1990). It therefore cannot justify a search of the data that is electronically stored on the phone. *United States* v. *Davis*, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011) ("[A] lawful inventory search does not authorize an officer to examine the contents of a cell phone."); *United States* v. *Wall*, 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008), *aff'd*, 343 F. App'x 564 (11th Cir. 2009) ("[T]he Government cannot claim that a search of text messages on [defendant's] cell phones was necessary to inventory the property in his possession. Therefore, the search exceeded the scope of an inventory search and entered the territory of general rummaging."); *United States* v. *Flores*, 122 F. Supp. 2d 491, 494 (S.D.N.Y. 2000) ("[N]either a calendar book nor a cellular telephone is a 'container' that has 'contents' that need to be inventoried for safekeeping in the traditional sense of those terms.").

The broad argument advanced by California and the United States in these cases would, if accepted by this Court, enable police officers to "rummage at will" among individuals' most sensitive personal information—the very types of information whose protection was a core purpose of the Fourth Amendment. That argument should be rejected by this Court here, as it was in *Gant*.

### C. The Court Should Reject An Exception To The Warrant Requirement Permitting Searches Of Digitally-Stored Information For Evidence Of The Offense Of Arrest.

The federal government urges the Court to recognize a new exception to the Fourth Amendment's warrant requirement that would allow searches of digitally-stored information on cell phones (and presumably any other portable electronic device) whenever an officer has "reason to believe that it contains evidence of the offense of arrest." 13-212 U.S. Br. 45. The Court should reject that argument and reaffirm that a warrant is required to search these large collections of highly personal information.

Although the government relies on *Gant*, that decision actually weighs against the government's argument. The Court there concluded that "*circumstances unique to the vehicle context* justify a search incident to a lawful arrest when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" 556 U.S. at 343 (emphasis added). It did not adopt the general rule urged by the government here, which would not be limited to the vehicle context but rather would apply across-the-board to any place an arrest occurs and to any item found on the individual's person.

That enormous expansion of the government's authority to conduct warrantless searches is contrary to both precedent and the principles underlying the Fourth Amendment.

The government's argument rests largely on *United States* v. *Rabinowitz*, 339 U.S. 56 (1950); see 13-212 U.S. Br. 16 (citing *Rabinowitz)*; *id.* at 46 (citing *Thornton* v. *United States*, 541 U.S. 615, 629 (2004) (Scalia, J., concurring) (relying on *Rabinowitz*)).

But *Chimel* expressly rejected that broad interpretation of *Rabinowitz*, stating that "*Rabinowitz* has come to stand for the proposition, *inter alia,* that a warrantless search 'incident to a lawful arrest' may generally extend to the area that is considered to be in the 'possession' or under the 'control' of the person arrested"; that *Rabinowitz* had been thus "limited to its own facts"; and that a broad construction of the decision was inconsistent with other decisions of this Court and not "supported by a reasoned view of the background and purpose of the Fourth Amendment." 395 U.S. at 759-760. Adopting the government's argument would therefore be inconsistent with *Chimel*.

Searches of digitally-stored information are a particularly inappropriate context in which to adopt a new exception to the warrant requirement, because such a search inevitably will allow police officers to rummage through a large volume of extremely personal information. As discussed above, that is the precise sort of search that led to the adoption of the Fourth Amendment's requirement of a warrant.

Moreover, the government never explains why a warrant requirement would be burdensome in this context. Where officers have secured the portable

electronic device, and there are no exigent circumstances, it should be possible to obtain a warrant in short order. *McNeely*, 133 S. Ct. at 1562-63.

A warrant also serves the important purpose of tailoring the scope of the officers' search of digitally-stored information to fit the justification for the search. See *Maryland* v. *Garrison*, 480 U.S. 79, 84 (1987) (explaining that Fourth Amendment requires that a warrant be limited "to the specific areas and things for which there is probable cause to search" in order to avoid "tak[ing] on the character of the wide-ranging exploratory searches the Framers intended to prohibit"). Given the large amount of sensitive personal information contained on these devices, it often will be appropriate to limit the search to the particular type of information to which the officers' probable cause relates.

The government appears to argue that the police officer's determination that there is reason to believe that the device contains evidence of the crime, and the officer's determination of the appropriate scope of the search, are sufficient substitutes for the judgment of a detached magistrate. But the Framers concluded otherwise, based on their experience with abuses of government investigatory authority, and therefore specifically included the warrant requirement in the text of the Fourth Amendment.

Given the particular importance of the warrant requirement in the context of searches of personal papers and other personal information, the absence of any demonstrated burden on law enforcement, and this Court's precedents, the government's argument should be rejected.

### D. A Bright-Line Rule Requiring A Warrant For Searches Of Digitally-Stored Information Will Be Much Easier For Officers To Apply Than Other Proposed Standards.

The Court has consistently recognized the benefits of bright-line rules in the Fourth Amendment context. "A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront." *Dunaway* v. *New York*, 442 U.S. 200, 213-214 (1979). "[I]f police are to have workable rules, the balancing of the competing interests * * * 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'" *Michigan* v. *Summers*, 452 U.S. 692, 705 n.19 (1981) (quoting *Dunaway*, 442 U.S. at 219-220 (White, J., concurring)).

Requiring a warrant for searches of digitally-stored information would provide clear guidance to police officers. Once the officers concluded that they wanted access to information stored on a portable electronic device, and the relevant information was not in plain view, they would know that a warrant is required (absent case-specific exigent circum-

stances).[31] Other proposed standards would create confusion and uncertainty.

*1. There Are No Clear Distinctions Between "Smart" And "Dumb" Cell Phones.*

No easily ascertainable set of characteristics separate "smart" from "dumb" cell phones—to the contrary the two categories overlap significantly. Thus, the TracFone Prepaid Cell Phone, sold at Walmart for $14.88, includes mobile web access, video recorder, instant messaging, an MP3 player, voice recorder with playback capability, a camera, text messaging capability, a calendar, and a phonebook that can hold 1,000 entries. *TracFone LG440G Cell Phone*, Walmart, http://perma.cc/RDR2-JCLY; see also note 6, *supra*.

Certainly phones are not labeled "smart" or "dumb." Police officers cannot be expected to stay abreast of the latest cell phone developments to distinguish quickly between the myriad of different phone models. And many recent "dumb" phones have the sleek design typically associated with smart phones.[32]

Moreover, cell phones are only one of the many categories of portable electronic devices to which police officers would have to apply this hazy distinc-

---

[31] The burden of obtaining a warrant is no greater in this context than it is in other contexts in which there is no exception to the general standard prescribed by the Fourth Amendment. And advances in technology have made it much easier to obtain a warrant expeditiously. *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562-1563 (2013).

[32] See, *e.g.*, Stephanie Mlot, '*Premium' Nokia 515 Feature Phone Unveiled*, P.C. Magazine (Aug. 28, 2013, 4:06 PM), http://perma.cc/N3ZJ-C8SQ.

tion. They also would have to be knowledgeable about different models of tablets, laptops, and digital cameras, among other devices.

Finally, any distinction along these lines would quickly become obsolete. As technology advances, production of today's "dumb" devices will cease, today's "smart" devices will become relatively "dumber," and new "smarter" smart devices will enter the marketplace.

Officers on the street simply could not keep themselves aware of the information needed to apply this distinction, assuming that some distinction between types of devices could even be delineated. The result would be rampant confusion.

*2. Permitting Law Enforcement Officers To Access Only Certain Types Of Digitally-Stored Information Is Wholly Impractical.*

Modern cell phones and other portable electronic devices do not limit a user's access to particular categories of information. To the contrary, the stored information is not compartmentalized and one of the purposes of the phone's applications is to link the various types of information to improve the phone's utility.

For example, "many of the most popular smartphone apps for Apple and Android devices— Twitter, Foursquare and Instagram among them— routinely gather the information in personal address books" for use in those apps.[33] The National Security Agency

[33] Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. Times (Feb. 15, 2012, 9:05 AM), http://perma.cc/VZP7-R4TR.

found that certain popular phone apps access sensitive personal information contained on the phone relating to location, age, gender, and sexual orientation.[34] Because data on the phone is so interconnected, a rule permitting police to search some subset of the information simply is not workable.

Moreover, permitting an officer to "look at" only the phone's call log opens the door to fishing expeditions. Police officers will claim that "in the process of" finding the call log they accidentally happened upon other information—a diary, photographs, text messages, emails—and that the other information is admissible on "plain view" grounds. The Court should not adopt a legal standard susceptible to such manipulation, particularly in light of the highly personal nature of the large amounts of information stored on these devices.

An additional flaw in this approach is that a police officer on the street, in the heat of the moment of arrest, often will not be able to determine whether the data he or she is accessing is stored on the electronic device or stored remotely on a server. The federal government acknowledges (No. 13-212 U.S. Br. 34-44) that the search-incident-to-arrest exception cannot justify searches of remotely-stored information. That fact weighs heavily against permitting warrantless searches of particular categories of information.

Apps on cell phones seamlessly integrate local and remotely stored data, making it all but impossi-

---

[34] James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, The Guardian (Jan. 28, 2014, 2:51 AM), http://perma.cc/3LKY-YDWR.

ble to tell where exactly the data displayed on the screen is coming from. In fact, official design principles for both Apple's iOS operating system for iPhones and Google's Android operating system *emphasize* a user experience that obfuscates the difference between local and remote data for the end user. See *iOS Human Interface Guidelines* 62 (2014), http://perma.cc/M5DA-24DR ("[P]eople shouldn't be faced with anything that encourages them to think about file metadata or locations[.]"); *id.* at 101-102 ("Ideally, users don't need to know where their content is located[.] * * * Avoid asking users to choose which documents to store in iCloud."); *Design Principles*, Android Developer, http://perma.cc/N534-576H ("Save what people took time to create and let them access it from anywhere. Remember settings, personal touches, and creations across phones, tablets, and computers.").

Some apps provide a live video feed into a person's home—and more. See, *e.g.*, Somak R. Das et al., *Home Automation and Security for Mobile Devices*. 2011 IEEE International Conference on Pervasive Computing and Communications Workshops 141, 141 (describing the design of a phone-app-based system that "operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video and records it for future playback, and finally manages operations on home appliances, such as turning ON/OFF a television or microwave or altering the intensity of lighting around the house"). Cf. *Kyllo*, 533 U.S. at 35-36 (discussing "imaging technology that could discern all human activity in the home").

An officer could not reliably determine whether, by opening an app, he was looking at a local copy of a

stored email or at emails stored remotely, or whether the personal pictures found were stored on the phone or were instead located on the user's private online photo album (or another individual's online photo album). Law enforcement officers will not be able to make a distinction that is designed by software developers to be essentially invisible.

*3. Distinguishing Between Searches At The Place Of Arrest And Searches At The Police Station Would Increase The Intrusion On Privacy Interests Protected By The Fourth Amendment.*

The petitioner in No. 13-132 suggests (Pet. Br. 44-53) that the Court could resolve that case by holding that a search conducted remotely from the time and place of arrest violates the Fourth Amendment. Whatever the legal merit of that proposition (compare *United States* v. *Edwards*, 415 U.S. 800 (1974)), a legal standard that permits searches at the time and place of arrest would open the door to warrantless searches of large volumes of highly personal information.

To begin with, such a standard would not impose any practical limitation on these searches. Police cars today typically are outfitted with laptop computers and other devices that can be used to download and search digitally-stored information. Thus, one global survey found that 44% of respondents "now extract mobile data in the field." *Trends shaping mobile forensics in 2014*, http://perma.cc/R8EA-GBP2.

A legal rule that permits police to search all digitally-stored data at the place of arrest without a warrant, but requires a warrant for any subsequent

search, would create a strong incentive *always* to search that information at the scene—and therefore is likely to produce more frequent warrantless searches of this personal information and therefore greater intrusions on the privacy interests protected by the Fourth Amendment.

## CONCLUSION

The judgment of the court of appeal in No. 13-132 should be reversed and the judgment of the court of appeals in No. 13-212 should be affirmed.

Respectfully submitted.

EUGENE R. FIDELL
*Yale Law School*
*Supreme Court Clinic*
*127 Wall St.*
*New Haven, CT 06511*
*(203) 432-4992*

ANDREW J. PINCUS
*Counsel of Record*
CHARLES A. ROTHFELD
MICHAEL B. KIMBERLY
PAUL W. HUGHES
*Mayer Brown LLP*
*1999 K Street, NW*
*Washington, DC 20006*
*(202) 263-3000*
*apincus@mayerbrown.com*

MARCH 2014