No. 13-132

IN THE
Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari to the
Court of Appeal of California,
Fourth Appellate District

BRIEF *AMICUS CURIAE* OF THE DKT LIBERTY PROJECT IN SUPPORT OF PETITIONER

Donald B. Mitchell, Jr.*
James H. Hulme
ARENT FOX LLP
1717 K Street, N.W.
Washington, DC 20036
(202) 857-6000
donald.mitchell@arentfox.com

*** Counsel of Record**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

Thomas Jefferson warned "the natural progress of things is for liberty to yield and government to gain ground." Letter to Edward Carrington, May 27, 1788. Mindful of this trend, The Liberty Project was founded in 1997 to promote individual liberty against encroachment by all levels of government and to defend the right to privacy. The not-for-profit Liberty Project advocates vigilance over regulation of all kinds, especially restrictions of individual civil liberties that threaten the reservation of power to the citizenry that underlies our constitutional system. The Liberty Project has participated as *amicus* in this Court several times in the past, including in cases raising similar issues, such as *Kyllo v. United States*, 533 U.S. 27 (2001).

This case concerns the fundamental right of citizens to privacy in their papers and communications, and in their homes. The smartphone is a computer, small in size but full in function, creating and holding private papers, and providing access via the Internet to the home. Because of The Liberty Project's long interest in privacy and in protection of citizens from government overreaching, it is well situated to provide this Court with additional insight into the issues presented in this case.

---

[1] The parties have consented to the submission of this brief; their letters of consent are on file with the Clerk. None of the parties or their counsel authored this brief in whole or in part and no one other than *amicus* and its counsel contributed money or services to the preparation of this brief.

SUMMARY OF ARGUMENT

The modern smartphone is a miniaturized computer that creates content, sends mail, stores private papers, accesses personal financial and medical information, and runs computer programs to accomplish specific tasks. Notably, smartphones now enable remote access to the user's home. Smartphone users create such content and enable such access with the reasonable expectation that it will remain private.

1. The Fourth Amendment attaches when a citizen has a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347 (1967). The Court has recognized that the "reasonable expectation of privacy" standard evolves with technology and that the rules it adopts must take account of systems that are both in use or in development. *Kyllo v. United States*, 533 U.S. 27 (2001). A large quotient of judicial humility is called for when making rules involving evolving technology.

2. Searches conducted without prior approval by a magistrate are per se unreasonable under the Fourth Amendment, subject only to a few well-delineated exceptions. *Coolidge v. New Hampshire*, 403 U.S. 443 (1971). The exceptions are carefully drawn and the burden is on those seeking an exemption to show the need for it. *Id.* Absent exigent circumstances, the threshold of the home may not reasonably be crossed without a warrant. *Payton v. New York,* 445 U.S. 573 (1980). And *Kyllo* makes clear that a "virtual" search using technology that discerns activity within the home is forbidden by the Fourth Amendment.

3. The search incident-to-arrest exception to the Warrant Clause no longer applies once the property to be searched comes under the exclusive control of the police. *United States v. Chadwick,* 433 U.S. 1, 15 (1977). If the police have probable cause to believe that the smartphone contains evidence of the crime of arrest, they may seize the phone and turn it off or otherwise secure it so that there is no risk of destruction of evidence while a warrant upon probable cause is obtained. This simple standard comports with the needs of law enforcement for clear, bright line rules.

THE MODERN SMARTPHONE IS A SMALL COMPUTER IN WHICH CITIZENS HAVE EXTRAORDINARY PRIVACY INTERESTS

The Smartphone is Ubiquitous.

The modern smartphone[2] has become ubiquitous. Ninety-one percent of American adults own some form of mobile phone.[3] More than three out of five adult women use a smartphone,[4] and among persons between the ages of 25 and 34 about 78% own a

---

[2] Within the category of "smartphone" we also include the even newer technology commonly known as the "tablet" — they perform essentially the same functions.

[3] *Cell Phone Activities 2013*, http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013 (last accessed Mar. 3, 2014). All Internet sites cited in this brief were last accessed on March 3, 2014, and this date is not repeated in each citation below.

[4] *Mobile Majority: U.S. Smartphone Ownership Tops 60%*, http://www.nielsen.com/us/en/newswire/2013/mobile-majority--u-s--smartphone-ownership-tops-60-.html.

smartphone.[5] And the percentages of smartphone users are increasing. Thus, when police encounter an adult citizen, they are also likely to encounter a smartphone. The issues raised in this case, therefore, are widespread — and are only likely to become more frequent, significant, and prominent.[6]

The Smartphone Is A Small Computer, And It Contains Intimate Information

The modern smartphone is much more than a telephone. Even a $9.99 "Tracfone" can create content — it can record pictures and video, send and receive text messages, browse the Internet, etc.[7] And more sophisticated devices can create content, store papers, access personal financial and medical information, serve as a repository for thoughts, run computer programs to accomplish specific tasks, and store information and images that the creator does

---

[5] *Id*.

[6] About half the States now permit drivers to show police digital insurance cards on their smartphones to verify insurance at traffic stops. A. Carrns, *More States Permit Digital Car-Insurance Cards*, NEW YORK TIMES (June 18, 2013), *available at* http://bucks.blogs.nytimes.com/2013/06/18/more-states-permit-digital-car-insurance-cards/?_php=true&_type=blogs&_r=0. The future questions lurk: Has the citizen voluntarily given up his expectation of privacy in the phone? May the officer manipulate or search the phone? Does the "brief" nature of the phone seizure justify some search? *Cf., United States v. Place,* 462 U.S. 696, 705-06 (1983).

[7] *E.g., LG 800G Prepaid Phone With Triple Minutes (Tracfone)*, http://www.amazon.com/LG-800G-Prepaid-Minutes-Tracfone/dp/B006E8MKZU/ref=sr_1_2?s=wireless&ie=UTF8&qid=1393431740&sr=1-2&keywords=tracfone+cell+phones.

not intend others to view or see. It is not uncommon for adults to carry intimate photos of a spouse or romantic partner on the device, with no intention that others will view the photos. A recent survey by computer security company McAfee reports that a *majority* of mobile device owners have used them to "send or receive intimate content including video, photos, emails and messages;" among the eighteen to twenty-four year old group, the percentage sending or receiving intimate content was seventy percent.[8] And almost half of smartphone users have stored intimate content received from another person on their smartphones.[9]

Smartphone users create or save such intimate content with the expectation that it is private and will remain private. Yet, once the device is in the hand of the police, the photos or other private information are available to be viewed, passed around, and even shared with the public. This occurred in Virginia, where the police (without a warrant) found intimate photos of an arrestee's girlfriend in "sexually compromising positions" on the arrestee's phone and then alerted other officers in the station house and "members of the public 'that the private pictures were available for their viewing and enjoyment.'"[10]

---

[8] *Study Reveals Majority of Adults Share Intimate Details Via Unsecured Digital Devices*, http://www.mcafee.com/us/about/news/2014/q1/20140204-01.aspx?culture=en-us&affid=0.

[9] *Id*.

[10] *Newhard v. Borders*, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009).

The Smartphone Is A Doorway Into The Home And A Repository Of Private Medical And Financial Papers

The fully enabled smartphone has become an extension of one's self and a window into the person, her life, and her home.[11]

Smartphones are miniaturized computers. They operate by allowing their users to select and add what are commonly referred to as "apps" — software programs that implement a particular function[12] — to the base operating system. Common apps allow people to access their bank accounts to move money and make payments, access medical records, select and read newspapers, shop online, pay for on-street automobile parking, buy travel tickets, create and store information about their daily routines, and access other computers or other devices connected to computers, including computers and devices located in the home, far from where the phone user may be located.

For example, with one click of an icon on a smartphone one may literally look into the home (or other location) by using the "iCam" app to view an

---

[11] As one psychologist has noted, the "smartphone is quickly becoming an extension of the human brain." S. Whitbourne, *Your Smartphone May Be Making You … Not Smart* (Oct. 18, 2011), http://www.psychologytoday.com/blog/fulfillment-any-age/201110/your-smartphone-may-be-making-you-not-smart.

[12] An "app" is "a self-contained program or piece of software designed to fulfill a particular purpose; an application, esp. as downloaded by a user to a mobile device." Google, "What is an app?".

Internet-connected camera installed in the home.[13] The most obvious use for these camera apps is to monitor your home. You can keep an eye on kids or pets while you are away, or keep an eye on the interior or exterior of the home when you are not there. Other home-related apps allow one to turn the lights and utilities on and off, monitor home security systems, and even prepare your bath, filling the bathtub to the homeowner's favorite combinations of temperature, depth and aroma.[14]

Other common services such as Google Docs and Apple's iWork allow one to create documents in the privacy of one's home or office and have them appear automatically on one's other devices — computers, smartphones and tablets — thus turning the mobile device into an extension of the home or office, a form of "digital home."

In addition to these uses, one can access confidential tax, banking, and investment records with the click of an icon on a smartphone. Almost thirty percent of smartphone users have used their device to check a bank balance or perform on-line

---

[13] The iCam app is available for iOS (Apple), Android, and Windows smartphones: http://skjm.com/.

[14] iTunes App Store, "Bathomatic," https://itunes.apple.com/us/app/bathomatic/id318150697?mt=8&ign-mpt=uo%3D4. In *Kyllo*, 533 U.S. at 38, this Court condemned technology that "might disclose … at what hour each night the lady of the house takes her daily sauna and bath;" now, searching her Bathomatic-enabled smartphone, the Government will know not just the time but her favorite aroma and the depth of her bubbles.

banking functions.[15] A smartphone user can also view medical records and treatment history with just one or two clicks. In other words, almost every human activity can be documented, monitored, evaluated, and viewed on one's smartphone — no matter how personal, intimate or trivial. The Apple App Store now has more than one million "apps" for almost every conceivable human activity.[16]

As one uses a smartphone, a great deal of additional data about the person is created and stored. Photos taken by the device contain not just the image, but metadata such as where and when the photograph was taken. Every time an iPhone user closes the built-in mapping application, the phone stores a screenshot, thus memorizing where the phone was at that particular time. As various apps are opened and closed, data is created and stored about what apps were opened, how long they were open and, frequently, what was done on them. Access to this data can pinpoint the location of the device and a great deal about the private activities engaged in by the user.

The Smartphone Is A Window Into The Person's Mind

Just as the smartphone has become an extension of the home and an access point to financial and medical papers, it also has become a window into a person's mind, goals, failures and successes.

---

[15] *See Cell Phone Activities, supra* n.3.

[16] S. Costello, *How Many Apps Are in the iPhone App Store*, http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm.

Already, a smartphone owner may use the device as a surrogate therapist.[17] "Moody Me" is an app that allows the user to track his or her mental states. "You can delve deeper into what's causing the mood with a list of relevant emotions, symptoms and events. Users who are taking medications can also note them in their daily mood entries. The app also creates graphs of moods over time so users can detect patterns."[18] A person grappling with depression may consult "depressioncheck" — an app that "is a state-of-the-art, research validated screen that in 3 minutes assesses your risk of depression, bipolar and anxiety disorders (including PTSD). After completing the short checklist you receive a personalized confidential report sharing how much burden these symptoms may be causing you."[19] Other apps allow a user to track sleep, stress and relaxation levels.[20] The totality of these entries creates a record of the person's mind and its inner workings, his thoughts, her feelings. If viewed, the app data would be a look directly into the person's

---

[17] E. Landau, *Smartphone apps become 'surrogate therapists'* (Sept. 22, 2012), http://www.cnn.com/2012/09/27/health/mental-health-apps/index.html.

[18] *Id*.

[19] iTunes App Store, "depressioncheck," https://itunes.apple.com/us/app/depressioncheck/id398170644.

[20] *See, e.g.,* S. Kiume, *Top 10 Mental Health Apps*, http://psychcentral.com/blog/archives/2013/01/16/top-10-mental-health-apps/; A. McCann, *Smartphone Shrink: 5 Apps To Help Your Mental Health*, http://www.popularmechanics.com/science/health/med-tech/smartphone-shrink-5-apps-to-help-your-mental-health#slide-1.

mental state, feelings, and beliefs — information that is at the heart of the expectation of privacy.

One of the more common uses for apps is to assist the user with nutrition, physical fitness, and other health-related management activities. The "Fitbit" app allows the smartphone user to track "steps taken, distance traveled, calories burned, stairs climbed and active minutes throughout the day," and then at night to track sleep patterns, restless periods, and awake periods; all of the data are then stored, analyzed, and available to be displayed on the smartphone.[21] There are numerous apps that allow a woman to track and record her ovulation and menstruation cycle.[22] And there are thousands of apps and other devices which allow the user to record her daily activities, including the details of each meal eaten, beverages consumed, steps taken, each beat of the heart, etc.[23]

While most smartphone users (at least now) take advantage of only two or three dozen of the available apps, the most common uses often involve the most personal information. In a word, the smartphone is an extension of a person's papers — her financial records, his medical records — and a doorway into

---

[21] *Push yourself further with Force™*, http://www.fitbit.com/force.

[22] *E.g.*, "Period Plus (Menstrual, Fertile, Ovulation, Calendar, Tracker, … for Women Cycle)," *available at* https://itunes.apple.com/us/app/id318894849?mt=8; "iPeriod Period Tracker Free - Menstrual Calendar," *available at* https://itunes.apple.com/us/app/id340757216?mt=8.

[23] *E.g.*, *The 64 Best Health and Fitness Apps of 2013* (Mar. 27, 2013), http://greatist.com/health/best-health-fitness-apps.

his or her mind, body, and home through the data stored or accessible on the device. It is, in many ways, nothing less than *home* — digital, but an extension of home nonetheless.

Much Data Available To The Smartphone Is Not Actually Resident On The Device

Smartphones have become so advanced and interconnected with the Internet that the data being viewed on the phone *is likely not even on the device*. Rather, by clicking on an icon, the user frequently causes the device to reach out to another computer to access and display the data, picture, etc. This other computer may be on what is commonly referred to as the "cloud."[24] *Or, it may be on or attached to another one of the user's computers in his or her home* — one that clearly could not be searched without a warrant. Just as clicking on the iCam icon causes the device to bring up a live-time view of whatever the remote camera is looking at, clicking on other icons may cause the device to display data that is actually stored on a remote computer.

Thus, a law enforcement officer examining a smartphone cannot tell whether he is inspecting the contents of the smartphone itself or, in reality, accessing a remote computer located in the owner's home or other location. Indeed, a police officer with access to the device who clicks the iCam icon will not

---

[24] "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet...." *United States v. Cotterman,* 709 F.3d 952, 965 n.12 (9th Cir. 2013) (en banc), *cert. denied,* 134 S. Ct. 899 (2014).

know if he is about to peer into the home until the image appears on the screen.[25]

Once Seized, Smartphones Can Be Secured Until A Warrant Is Obtained

As soon as a smartphone is in the hands of the police, the arrestee cannot directly remove any data, and it may be secured until a warrant is obtained with no risk of loss of data or potential evidence.

Forensic specialists have reached a consensus as to the best methods to secure a smartphone once it has been seized. According to the National Institute of Science and Technology: "Two basic methods for isolating the mobile device from radio communication ... are to either place the device in airplane mode, turn the device off, or lastly place the device in a shielded container."[26] Forensic specialists in the United Kingdom agree: "Isolate the device from network – this may be achieved by one of the following techniques: Turn device off at the point of

---

[25] The United States, in its brief in *Wurie,* No. 13-212, concedes that the search incident-to-arrest "doctrine does not permit officers to use the phone's Internet connection to access files stored elsewhere." U.S. Br. at 10; *see also id.* at 43-44. The problem, as set forth in the text, is that the officer *cannot tell* that his search is actually accessing files stored elsewhere. Thus, for example, even email or voice mail accessed via a smartphone is usually not *on* the phone, but on the cloud.

[26] Nat'l Inst. of Standards and Tech., *Guidelines on Mobile Device Forensics*, Special Pub'n 800-101 (Draft, Sept. 2013), at 30 , *available at* http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

seizure ... Place device in shielded container/bag."[27] Finally, the Scientific Working Group on Digital Evidence — which is chaired by representatives of the U.S. Secret Service and the FBI, and is composed of representatives of all federal law enforcement agencies — states: "If the phone is unable to be processed immediately, turn off phone, remove battery if practical, and do not turn it back on."[28] Tellingly, in its brief in *Wurie*, No. 13-212, the United States does *not* argue that turning the phone off does not preserve the data on it; instead, the United States argues that turning the phone off may mean that a password will be required to access its data, and that that would make law enforcement less convenient. *E.g.,* U.S. Br. in *Wurie,* at 34-37.

Thus, the simple and effective method of securing a smartphone is to turn it off. It may then be turned on in a secure location that is protected from outside interference, eliminating the threat of remote wiping. As noted above, another way to secure a device is to place it in a shielded container — a simple bag made of materials designed to prevent the device from communicating or being remotely wiped, generically

---

[27] *Good Practice Guide for Computer-Based Electronic Evidence (Official Release Version)*, Association of Chief Police Officers, at 46, *available at* http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf .

[28] *SWGDE Best Practices for Mobile Phone Forensics*, at 5 (Feb. 11, 2013), *available at* https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20V2-0.

called a "Faraday Bag."[29] Such bags are widely available at low cost for use on smartphones, tablets, laptops, and any other device that communicates over cellular, WiFi, satellite, or any other radio frequency network.[30] Once secured, any information on the device will be preserved until it may be forensically examined. In other words, once secured, the smartphone is no different from a desktop computer that is seized with a warrant on probable cause and held for a forensic examination.[31]

ARGUMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…." U.S. Const., amend. IV. "[T]he most basic constitutional rule in this area is that 'searches conducted ... without prior approval by judge or magistrate, are per se unreasonable under

---

[29] *See* http://www.faradaybag.com for but one source of such bags.

[30] *E.g.*, *Black Hole Faraday Bag - RF Signal Isolation for Forensics, Standard Window Size*, http://www.amazon.com/Black-Hole-Faraday-Bag-Isolation/dp/B0091WILY0.

[31] It has been suggested, incorrectly, that turning a smartphone off does not really turn it off because it could contain a "roving bug" that would allow it to operate even when the device is "off." *E.g., United States v Flores-Lopez*, 670 F.3d 803, 808 (7th Cir 2012) (citing *United States v. Tomero*, 471 F. Supp. 2d 448, 450 & n.2 (S.D.N.Y. 2007)). The *Flores-Lopez* court misreads *Tomero*. In *Tomero*, the "roving bug" was a court-authorized wiretap installed by the FBI which made the phone's microphone constantly active as an area listening device.

the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions.'" *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). "The exceptions are 'jealously and carefully drawn,'" and "'*[t]he burden is on those seeking the exemption to show the need for it*.'" *Id.* at 455 (emphasis added, footnotes and citations omitted).

The Fourth Amendment Protects Citizens' Privacy Interests In Their Smartphones

In his venerable and vindicated dissent in *Olmstead v. United States*, Justice Brandeis said that a constitutional provision such as the Fourth Amendment must have the "capacity of adaptation to a changing world." 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting). "In the application of a Constitution, therefore, our contemplation cannot be only of what has been but of what may be." *Id.* at 473 (citation omitted). *Accord United States v. Chadwick,* 433 U.S. 1, 9 (1977), *abrogated in part on other grounds, California v. Acevedo*, 500 U.S. 565 (1991) ("the Framers ... intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth").

In order to prevent the creeping loss of liberty about which Thomas Jefferson warned, *see* Interest of *Amicus Curiae, supra,* "Constitutional provisions for the security of person and property are to be liberally construed." *Byars v. United States*, 273 U.S. 28, 32 (1927). As Justice Bradley stated for the

Court in *Boyd v. United States*, 116 U.S. 616, 635 (1886):

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance.

The principles of the Fourth Amendment "apply to all invasions on the part of the government … of the sanctity of a man's home *and the privacies of life*." *Id.* at 630 (emphasis added). *Accord Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) ("We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property….").

Thus it is black letter law that the Fourth Amendment attaches when a citizen has a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 351-52 (1967); *id.* at 360-61 (Harlan, J., concurring) ("there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

Crucially for this case, the Court has recognized that the "reasonable expectation of privacy" standard

evolves with technology. "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo,* 533 at 33-34.

> Reversing that [*Katz*] approach would leave the homeowner at the mercy of advancing technology…. While the technology used in the present case was relatively crude, *the rule we adopt must take account of more sophisticated systems that are already in use or in development*.

Id. at 35-36 (emphasis added).

The warrant requirement serves important and fundamental purposes, and abates the creeping loss of liberty otherwise inherent in the competitive activity of policing. Justice Jackson, speaking for the Court in *Johnson v. United States*, 333 U.S. 10 (1948), perhaps said it best:

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.... When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.

Id. at 13-14. *Accord Katz,* 389 U.S. at 358-59 ("bypassing a neutral predetermination of the scope

of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police") (citation and internal quotations omitted); *McDonald v. United States*, 335 U.S. 451, 455-56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.").

Good faith, good policing technique, and even actual probable cause do not excuse the requirement of a warrant.

> In the absence of [the judicial warrant procedure] safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," for the Constitution requires "that the deliberate, impartial judgment of a judicial officer ... be interposed between the citizen and the police."

Katz, 389 U.S. at 356-57 (citations omitted). *Accord Arkansas v. Sanders,* 442 U.S. 753, 758 (1979), *abrogated on its facts, California v. Acevedo*, 500 U.S. 565 (1991). As Chief Justice Burger stated for the Court:

> Once a lawful search has begun, it is also far more likely that it will not exceed proper bounds when it is done pursuant to a judicial authorization 'particularly describing the place

> to be searched and the persons or things to be seized.' Further, a warrant assures the individual whose property is searched or seized of the lawful authority of the executing officer … and the limits of his power to search.

Chadwick, 433 U.S. at 9 (citation omitted).[32]

All of these Fourth Amendment concerns are sharpened and heightened when intrusion into the home is at issue, as is — and will increasingly be — the case with smartphone searches. Resistance to the British general warrants and writs of assistance "established the principle which was enacted into the fundamental law in the 4th Amendment, that a man's house was his castle, and not to be invaded by any general authority to search and seize his goods and papers." *Weeks v. United States*, 232 U.S. 383, 390 (1914); *accord Payton v. New York,* 445 U.S. 573, 597 n.45 (1980) ("'A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle....'," *quoting* 2 Legal Papers of John Adams 142 (L. Wroth & H. Zobel eds. 1965)). *See generally* Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 905, 907-12 (2010).

> The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an

---

[32] The need for assurance of "proper bounds" and "the limits of his power to search" is exemplified by cases like *Newhard v. Borders*, *supra* n.11.

> individual's home — a zone that finds its roots in clear and specific constitutional terms: "The right of the people to be secure in their ... houses ... shall not be violated." … [T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.

Payton, 445 U.S. at 589-90 (citation omitted). These principles apply, too, even to what some might consider a *de minimis* intrusion. *Kyllo,* 533 U.S. at 37 ("protection of the home has never been tied to measurement of the quality or quantity of information obtained" because "[i]n the home … *all* details are intimate details, because the entire area is held safe from prying government eyes").

And *Kyllo* makes clear that even a "virtual" search — one using technology from outside the home that discerns activity within the home, like the thermal imaging device in that case — is forbidden by the Fourth Amendment. *Id.* at 40. All searches that access the privacy of the home without a warrant are forbidden, whether the police physically cross the threshold or enter the curtilage or not. *Id.* It does not matter the technology: Whether the technology is a telescope or thermal imaging — or the iCam app — the result is the forbidden.

Smartphones Have Been Recognized As A Doorway Into The Person, The Mind, And The Home.

The U.S. Department of Justice readily acknowledges that "cell phones increasingly resemble

computers…."[33] Not surprisingly, virtually every court to address the issue has also found that modern smartphones combine features and have capabilities that previously would only be found in a library or office. *E.g., United States v Flores-Lopez*, 670 F.3d 803, 805 (7th Cir. 2012) ("a modern cell phone is a computer"); *Cotterman*, 709 F.3d at 964 ("Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails"); *Smallwood v. Florida*, 113 So. 3d 724, 732 (Fla. 2013) ("many people now store documents on their equipment that also operates as a phone that, twenty years ago, were stored and located only in home offices, in safes, or on home computers").

Modern smartphones have, for many people, effectively *replaced* desks and drawers and diaries, and contain or have access to the core secrets of their family, health, romantic, professional and financial lives that were formerly stored safely within the home — and which, undoubtedly, are subject to the warrant requirement when stored there. The First Circuit recognized this point in *United States v. Wurie,* 728 F.3d 1, 8 (1st Cir. 2013), *cert. granted,* No. 13-212, the companion case in this Court:

---

[33] *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. Dep't of Justice, Criminal Division, Computer Crime and Intellectual Property Section (2009), at 34 n.6, *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

> That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records.... *It is the kind of information one would previously have stored in one's home and that would have been off-limits* to officers performing a search incident to arrest. *See Chimel [v. California],* 395 U.S. 752 [(1969)].

(Emphasis added.) *See also Cotterman,* 709 F.3d at 964 ("This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'"); *Schlossberg v. Solesbee*, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) ("Electronic devices such as [a] digital camera hold large amounts of private information, entitling them to a higher standard of privacy."); *United States v. Park*, No. CR-05-375-SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) ("Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations").

Much ink has been spilled about whether smartphones are "containers" associated with an arrestee in a misguided (albeit understandable) effort to shoehorn this new technology into the search incident-to-arrest case law developed in the bygone days of paper, when a person could only bring with him the tangible property he could carry. *Compare, e.g., United States v. Finley,* 477 F.3d 250, 260 (5th Cir. 2007), and *California v. Diaz*, 244 P.3d 501, 507 (Cal. 2011) (each finding phone was a "container" and thus allegedly subject to search

under *New York v. Belton,* 453 U.S. 454 (1981)), *with United States v. Park*, 2007 WL 1521573, at *1 ("a modern cellular phone, which is capable of storing immense amounts of highly personal information, is properly considered a 'possession within an arrestee's immediate control' rather than as an element of the person"). But aside from the dubious *factual* determination that a smartphone would be a *Belton* container — since *Belton* states that a "container" is an "object capable of holding another object," 453 U.S. at 460 n.4, and a smartphone holds no "object" at all — the container analysis misses the *reality* of the technology and the constitutional privacy implications of citizens' uses of their smartphones.

The more recent decisions have begun to respect the *reality* that the nature of the smartphone means it cannot be shoe-horned into pre-digital boxes. *See, e.g., Smallwood*, 113 So. 3d at 732 ("the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity cigarette packet in *Robinson,* not only in the ability to hold, import, and export private information, but by the very personal and vast nature of the information that may be stored on them or accessed through the electronic devices"); *id.* at 732-33 ("In our view, attempting to correlate a crumpled package of cigarettes to the cell phones of today is like comparing a one-cell organism to a human being…. The cell phones of today have a greater capacity not just in the *quantity* of information stored, but also in the *quality* of information stored"); *Texas v. Granville*, __ S.W.3d __, 2014 WL 714730, at *6 (Tex. Crim. App. Feb. 26, 2014) ("clothing [like in *Edwards*] does not contain private banking or medical information and records;

it does not contain highly personal emails, texts, photographs, videos, or access to a wide variety of other data about the individual citizen, his friends and family. Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once"); *Cotterman*, 709 F.3d at 964 ("[t]he private information individuals store on digital devices — their personal 'papers' in the words of the Constitution — stands in stark contrast to the generic and impersonal contents of a gas tank"); *Schlossberg*, 844 F. Supp. 2d at 1169 ("[c]onsideration of an electronic device as a 'container' is problematic.… In order to carry the same amount of personal information contained in many of today's electronic devices in a container, a citizen would have to travel with one or more large suitcases, if not file cabinets"). *See also Ohio v. Smith*, 920 N.E.2d 949, 953-54 (Ohio 2009), *cert. denied,* 131 S. Ct. 102 (2010) ("The state argues that … a cell phone is akin to a closed container and is thus subject to search upon a lawful arrest. We do not agree with this comparison").

And as technology has advanced, the devices have become even less like "containers." No longer do the devices simply "contain" information within them on an internal microchip — which is, after all, the underlying factual (and etymological) premise for the faulty "container" analogy. Instead, they now provide access via the "cloud" and Internet to other computers *not "contained" in the phone, and even to the home. See Wurie,* 728 F.3d at 8 ("modern cell phones provide direct access to the home….; iPhones can now connect their owners directly to a home computer's webcam, via an application called iCam"); *Cotterman,* 709 F.3d at 965 ("[t]he digital device is a

conduit to retrieving information from the cloud, akin to the key to a safe deposit box. Notably, although the virtual 'safe deposit box' does not itself [travel with its carrier or the phone], it may appear as a seamless part of the digital device…. With access to the cloud … a traveler's cache is just a click away from the government"). It is as if Robinson's cigarette pack contained a key to his home or to a safety deposit box instead of capsules of heroin. No one would credibly argue that the police, having located the key, could simply use it to enter his home or safety deposit box without a warrant.

Citizens Have A Reasonable Expectation Of Privacy In The Information On, Or Accessible By, Their Smartphones

It is undisputed that citizens have a significant constitutional privacy interest in the contents within (on the chips of) their smartphones, *and* in their data and personal information on the cloud and other locations external to the phone that may be accessed remotely by those devices. As this Court recognized in *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010), "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."

The papers citizens store or access on their smartphones are often also expressive material, protected by First Amendment principles as well. As this Court has recognized, there are "special constraints upon searches for and seizures of material arguably protected by the First Amendment." *Lo-Ji Sales, Inc. v. New York,* 442 U.S. 319, 326 n.5 (1979). When searching First

Amendment protected areas, even searches *with* a warrant require special and careful limitation. *Zurcher v. Stanford Daily,* 436 U.S. 547 (1978). Such careful limitation is impossible in searches conducted by "competitive" police officers incident to arrest.

It is inconceivable that the privacy of the home, or a person's bank or financial or medical records — otherwise immune to seizure without a warrant — could be lost to Government merely by virtue of a citizen's use of the software and wireless amenities of modern life on a portable digital device. The devices are, after all, legal, and not themselves contraband. It is irrational that a person should lose constitutional protections available in the pre-digital world for her papers simply because technology now allows her to carry those papers, or a digital key to those papers, with her.[34] In this light, the devices are simply a *digital home,* or a digital extension of the home.

Each of the individual items of communications data commonly available on smartphones have been found to be entitled to protection in their pre-digital form. Over 100 years ago this Court recognized that private mail correspondence was constitutionally

---

[34] *Accord Smallwood,* 113 So. 3d at 738 ("allowing law enforcement to search an arrestee's cell phone without a warrant is akin to providing law enforcement with a key to access the home of the arrestee. Physically entering the arrestee's home office without a search warrant to look in his file cabinets or desk [on the one hand], or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone [on the other], is essentially the same for many people in today's technologically advanced society").

protected under the Fourth Amendment even when the letter in question was placed in the public mail service. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles."). No different rule should apply to email simply because a person carries them on his smartphone.[35] Similarly, *Katz* recognized that voice communications were protected. *Katz v. U.S.*, 389 U.S. at 352. No different rule should apply to modern text messaging — frequently in practice a form of back-and-forth communication equivalent to a voice call — simply because a person chooses to use the keyboard on her phone instead of the mouthpiece in a phone booth to engage in that conversation. The typical computer and its Internet browsing history, too, are protected from search without a warrant. *See United States v. Payton*, 573 F.3d 859, 861-62 (9th Cir. 2009) (search of computer not expressly authorized by warrant is not a reasonable search). No different rule should compromise the privacy interest in a citizen's Internet activity simply because it occurs on a portable computer like a smartphone or a tablet instead of the desktop computer in one's home or office.

---

[35] The justices of the Florida Supreme Court observed that they, too, had privacy interests in the email accounts on their cell phones. *Smallwood*, 113 So. 3d at 733 ("Indeed, even justices on this Court routinely use cellular phones to access Court email accounts, and highly confidential communications are received daily on these electronic devices.").

A rule making smartphones freely searchable upon arrest would mean that any citizen committing an arrestable offense could have his most private papers and information viewed by the arresting officer without any prior judicial involvement. The Courts that wrote *Robinson, Edwards* and *Belton*[36] — all, notably, in the pre-digital era — could not have foreseen a world in which almost everyone would be carrying on their person an item containing their most personal papers and access to their home, rather than mere tangible physical evidence. Those cases should not be applied to searches of clearly distinct digital technology.

Absent Exigent Circumstances, A Warrant Should Be Required To Search A Smartphone

There is, in fact, no need to contort search incident-to-arrest law either to protect the government's interest in police safety and law enforcement or citizens' interests in protecting their reasonable expectation of privacy. In our view, proper application of the rationale that underlies the search-incident-to-arrest exception to the warrant requirement, and proper application of the cases themselves, easily resolves the issue in favor of respecting the citizen's reasonable expectation of privacy, and without harming the government's interest in law enforcement.

---

[36] *United States v. Robinson,* 414 U.S. 218 (1973); *United States v. Edwards*, 415 U.S. 800 (1974); *New York v. Belton,* 453 U.S. 454 (1981).

In *Chimel v. California*, 395 U.S. 752, 762-63 (1969), the Court held that the "principle" which "marks [the exception's] proper extent" is that "[w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons" and that "[i]n addition, 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*." (Emphasis added.) *Accord Arizona v. Gant*, 556 U.S. 332, 339 (2009) (quoting *Chimel* and adding emphasis to *Chimel's* "in order to" clauses).

But when the circumstance that justifies this *exception to the general rule* that a warrant upon probable cause is always required disappears, so does the exception. "In our view, when no [other] exigency is shown to support the need for an immediate search, *the Warrant Clause places the line at the point where the property to be searched comes under the exclusive dominion of police authority*." *Chadwick*, 433 U.S. at 15 (emphasis added). *Accord Gant,* 556 U.S. at 339 ("If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, *both justifications for the search-incident-to-arrest exception are absent* and the rule does not apply") (emphasis added). In *Gant,* the Court emphasized the need for "the scope of a search incident to arrest" to be "commensurate with its purposes." *Id*.

Thus, the obvious solution *when the police have probable cause to believe that the smartphone contains evidence of the crime of arrest* is for the police simply to seize the phone and turn it off or otherwise secure it so

that there is no risk of loss or destruction of evidence while a warrant upon probable cause is obtained.[37]

To be clear, the police may not seize all smartphones as a matter of course while they decide whether to seek a warrant to search the phone. They may seize a phone consistently with the Fourth Amendment only when they have *probable cause* (not just a reasonable suspicion) to believe that the phone contains evidence *of the crime of arrest.* The "probable cause" threshold for seizing the phone, even incident to arrest, is well-established. *See e.g., United States v. Place,* 462 U.S. 696, 701 (1983) ("[w]here law enforcement authorities have probable cause to believe that a container holds … evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if … some other recognized exception to the warrant requirement is present," citing, *inter alia, Chadwick*). That probable cause

---

[37] Nothing about applying the usual Fourth Amendment rule and requiring a warrant in order to search smartphones incident to arrest would eliminate or modify the *alternative* "exigent circumstances" exception to the warrant requirement. For example, even though police may not search a home without a warrant, true exigency is an exception to that rule. *E.g., Brigham City v. Stuart,* 547 U.S. 398, 403-04 (2006) ("need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency"). We do not foreclose the possibility of a similar exigency exception for smartphones when, for example, it is believed that the smartphone contains information about the location of a kidnapped child, or may contain a triggering mechanism for a bomb.

standard recognizes the citizen's interest in continued possession of his smartphone and its monetary value. *Id.* at 706, 709-10 (specifically holding that the lesser "reasonable suspicion" standard justifies only a "brief" seizure of property, and that a seizure even for ninety minutes pending receipt of a warrant requires probable cause); *compare Illinois v. McArthur*, 531 U.S. 326, 334 (2001) (seizure with probable cause for two hours, pending arrival of warrant, permitted).[38] And *Gant* makes clear that it is "evidence relevant to the crime of arrest" that the police are entitled to search for, and that the search-incident-to-arrest exception does not authorize broad investigatory searches for evidence of *any* crime the arrestee might have committed. 556 U.S. at 343. *See also id.* ("In many cases, as when [the defendant] is arrested for a traffic violation, there will be no reasonable basis to believe the vehicle [or other property within the

---

[38] As a practical matter, if a custodial arrest is effected and the arrestee has the phone on his person when he is put into the police car or brought to the local jail, the phone may be *seized* and removed from his possession and inventoried on the same basis and under the same procedures as other property is taken from an arrestee during booking and incarceration. Even when properly seized at that time, however, it may not be *searched* without a warrant. *Sanders,* 442 U.S. at 766 ("Where … the police … lawfully have … secured [arrestee's property], they should delay the search thereof until after judicial approval has been obtained."); *Texas v. Granville*, 2014 WL 714730, at *7 (search of cell phone after placement in jail property room requires warrant). But if the phone is not on the arrestee's person — for example, it is on the passenger seat or on his desk or nightstand or some other nearby location — it may only be seized with probable cause. *U.S. v. Place*, 462 U.S. at 701.

control of the arrestee, like a smartphone] contains relevant evidence.").

The simple standard proposed here — which we believe is required by the Fourth Amendment — also comports with the needs of law enforcement for clear, bright line, and practical rules. As this Court has repeatedly held, 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, 213-14 (1979). This Court has therefore rejected both "inherently subjective and highly fact specific" rules that require "ad hoc determinations on the part of officers in the field" in favor of clear ones that will be "readily understood by police officers." *Thornton v. United States,* 541 U.S. 615, 623 (2004). *See also Belton,* 453 U.S. at 458 ("A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions … may be literally impossible of application by the officer in the field"). Such a rule is especially called for in the digital device field. *Schlossberg*, 844 F. Supp. 2d at 1170 ("it is impractical to distinguish between electronic devices…. It would require officers to learn and memorize the capabilities of constantly changing electronic devices.").

A case-by-case approach allowing searches of some smartphone files or directories but not others based on the reasonableness of the individual officer's particularized inferences in any given case — for example, recent call logs are okay, but emails and iCam apps are not, while text messages depend on how recently they were sent or received — would

result in exactly the "inherently subjective and highly fact specific" set of rules the Court has warned against. *Thornton*, 541 U.S. at 623. Such a rule would be both extremely difficult for officers in the field to apply and open to questions of when the line has been improperly crossed and when protected information has been accessed. Of the two available simple rules — [1] seize the phone with probable cause and obtain a warrant to search it, or [2] search it every time without a warrant — the latter is quite obviously overbroad and inconsistent with Fourth Amendment interests.

A large quotient of judicial humility is called for when making rules about evolving technology, for if anything is clear it is that we cannot see the future nor foresee the digital (or other?) types of devices the minds of scientists will create. Citing its earlier errors, this Court recognized in *Quon*, 560 U.S. at 759, that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. *See, e.g., Olmstead v. United States,* 277 U.S. 438 (1928), overruled by *Katz v. United States,* 389 U.S. 347, 353 (1967)."

> Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations.... Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.

Id. See also United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring):

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. [Citation omitted.] This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. … I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.

At bottom, the argument of California in this case (and of the United States in *Wurie*) fails because it allows the *Chimel* exception to swallow the Fourth Amendment warrant rule. Stripped of its legal verbiage, the United States's argument is both arrogantly dismissive of citizens' privacy interests[39] and based on expedience and convenience, neither of which justify circumventing the Warrant Clause. There is no true exigency in these cases once the police have possession of the smartphone. It is not a weapon, and the arrestee cannot destroy any evidence. And the over-hyped fear of "remote wiping" is "truly theoretical," *Wurie,* 728 F.3d at 11,

---

[39] *E.g.,* U.S. Br. in *Wurie,* at 3 (describing smartphones as "pervasive instrumentalities of crime"); *id.* at 30 (describing phones as "critical tools in the commission of crimes" that will "only become more useful in the commission of criminal offenses"). As Appellant's Brief points out in its first sentence, most people who are arrested are not "are never convicted of any crime" and are therefore not "criminals."

and nonexistent in the real world,[40] and can be obviated by two simple expedients: turn the phone off or put it in a shielded bag. *See also Wurie,* 728 F.3d at 11 (suggesting three options). The burden is on the Government, as the proponent of the exception to the warrant requirement, to demonstrate a *real* and exigent problem, not a "truly theoretical" possibility, that requires an exception to warrant requirement of the Fourth Amendment.[41] "[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." *Mincey v. Arizona,* 437 U.S. 385, 393 (1978).

CONCLUSION

For the reasons set forth above, we believe that warrantless cell phone data searches are *categorically* unauthorized under the search-

---

[40] It is notable that the brief of the United States in *Wurie,* No. 13-212, spends four pages, U.S. Br. at 37-41, discussing numerous hypotheticals about how a smartphone might be or could be remotely wiped, *yet fails to cite a single instance of remote wiping ever having actually occurred* after a smartphone was seized by the police. Given that "[t]he burden is on those seeking the exemption [from the Warrant Clause] to show the need for it, *Coolidge*, 403 U.S. at 455, the Government's failure to identify even a single instance of "remote wiping" actually occurring — especially after the First Circuit called out the threat as "truly theoretical" — is fatal to its effort to square smartphone searches with *Chimel's* rationale.

[41] Given the rapid speed with which warrants may now be obtained, *see Missouri v. McNeely,* 133 S. Ct. 1552, 1561-62 (2013) (noting that "telecommunications innovations" now "allow for the more expeditious processing of warrant applications"), the inconvenience and risk to law enforcement should be minimal.

incident-to-arrest exception. If the police have probable cause to believe that the smartphone contains evidence of the crime of arrest, they may seize the phone and turn it off or "bag it" so that there is no real risk of loss or destruction of evidence while a warrant upon probable cause is obtained.

Respectfully submitted,

Donald B. Mitchell, Jr.
James H. Hulme
ARENT FOX LLP
1717 K Street, N.W.
Washington, DC 20036
(202) 857-6000
donald.mitchell@arentfox.com

Dated: March 10, 2014