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 California Court of Appeal, Fourth District

BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND THE BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW AS AMICI CURIAE IN SUPPORT OF PETITIONER

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NAT'L ASS'N OF CRIMINAL DEFENSE LAWYERS
1501 K Street, N.W.
Washington, D.C. 20005

BRONSON D. JAMES*
BRONSON JAMES LLC
522 N.W. 23rd Ave.
Portland, OR 97210
(503) 943-6876
bj@bronsonjames.com

MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
161 Ave. of the Americas,
New York, NY 10013

Counsel for Amici Curiae

* Counsel of Record

March 10, 2014

TABLE OF CONTENTS

TABLE OF CONTENTS—continued

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES—continued

TABLE OF AUTHORITIES—continued

COURT DOCUMENT

OTHER AUTHORITIES

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

INTEREST OF AMICI CURIAE[1]

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

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

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and limits on executive power in the fight against terrorism. The Center's Liberty and National Security (LNS) Program fights to ensure that our nation's commitment to national security respects constitutional values and the rule of law through innovative policy recommendations, litigation and public advocacy. The

---

[1] Both parties have filed blanket consent for amicus appearance in this matter. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. This brief does not purport to convey the position of NYU School of Law. It was written with the assistance of Amos Toh, Katz Fellow at the Brennan Center.

Brennan Center is particularly concerned with domestic counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and their effects on privacy and First Amendment freedoms. As part of this effort, the Center has published a series of reports on how law enforcement and intelligence agencies collect, share and retain information about Americans for national security purposes. *See* Michael Price, *National Security and Local Police* (2013); Rachel Levinson-Waldman, *What the Government Does with Americans' Data* (2013); Emily Berman, *Domestic Intelligence: New Powers, New Risks* (2011). The Center has also filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

SUMMARY OF THE ARGUMENT

Amici encourage this Court to prohibit the warrantless search of cellphones incident to arrest. Both the technical capacity of these devices to store great volumes of information, and the deeply private manner in which smartphones have become integrated into all aspects of daily living, create a significant privacy interest in their contents.

The search incident to arrest doctrine is governed by the rationale set forth in *California v. Chimel*. *Chimel's* twin exigencies, the need to protect officer safety, and the need to secure perishable evidence, are not present in the context of phone data. Cellphone data poses no threat to officer safety, and once

the phone has been reduced to police control, any risk of data loss is negligible.

Moreover, unlike in the context of vehicle searches, limiting a search to evidence related to the crime of arrest is unworkable with respect to cellphones. The nature and quantity of data on cellphones will mean that law enforcement will always be able to draw a connection between the offense of arrest and the phone, rendering a *Gant* limit a nullity. And practically, it is impossible for an officer in the field to conduct an appropriately limited search of digital data.

ARGUMENT

I. Mobile Computing Devices Like The Modern Smartphone Are Unique.

The Fourth Amendment is not blind to the advances of modern living. What is a reasonable search under the Fourth Amendment is a function of the privacy that society attaches to the place or object searched. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring). Reasonableness is not fixed to a particular technology level, unable to move beyond footlockers and cigarette packs, leaving the citizenry at the "mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001). Rather, as technology advances, and society's use of that technology creates new privacy expectations, what is reasonable is viewed anew.

A. The Capacity Of Mobile Computing Devices Renders Analogies To Physical Containers Inapplicable.

Any smartphone is capable of storing digital information locally, meaning that the physical device is the repository of the information. It is when we are discussing localized storage that analogizing these

devices to containers is even possible. However, the volume of information stored strains that analogy.

Current models of smartphones, such as the Apple iPhone and Samsung Galaxy S4 have 64GB (gigabytes) of localized storage. And storage capacity of models continues to expand with each new iteration.

In 2009, data storage manufacturers announced the development of the next-generation data storage architecture for phones, SDXc (Secure Digital Extended Capacity). The iPad2, one of the first devices to employ SDXc, is available in a 128 GB configuration. And SDXc is expected to push iPhones and other smartphones into the area currently reserved for laptop computers: the terabyte. Smartphones with storage in the 1-2 TB range are expected within this decade.[2] To place that number in perspective, a 1 TB phone could contain 120 hours of DVD-quality video, 720 hours of audio recordings, 22,200 high-res color photographs, 6,300,000 pages of MS Word documents and 97 million emails *all at once*, and still only be three-quarters full.[3]

With SDXc as the new storage architecture standard, individuals will truly have the capacity to store

---

[2] *See* Gary Krakow, *Smartphones, Meet the Terabyte*, The Street (Feb. 17, 2009), http://www.thestreet.com/story/10464195/smartphones-meet-the-terabyte.html; *and Terabyte Capacity for Smartphones*, Telecomasia.net (Feb. 16, 2009), http://www.telecomasia.net/content/terabyte-capacity-smartphones-0.

[3] Determining digital storage capacity is simply a mathematical calculation. To aid in that calculation, Petitioner refers this Court to a number of data storage computational aids online. *See, e.g, Data Capacity Converter Online*, Unit Converter, http://www.unitarium.com/data (last visited Mar. 7, 2014); *or Pages in a MB/GB e-Discovery Calculator*, Lexbe, http://www.lexbe.com/hp/Pages-Megabyte-Gigabyte.aspx (last visited Mar. 7, 2014).

an entire lifetime's data in their pocket. Videos of one's wedding, the birth of one's children, and every family reunion and school performance will easily fit on the device. Assuming 10 one-minute voicemails a day, everyday, the phone will hold over eleven years of voicemail messages. If you took three photographs of your child everyday of his life, from birth through high-school graduation, they would all fit on the phone with room to spare. It would easily contain not just every document you authored, but every page of every document you have ever read. Finally, it would hold every email and text message you have ever received or sent – *for your entire lifetime*.

Even though the capacity of localized storage strains traditional human conceptualizations of size, it is dwarfed by a cellphone's secondary storage mechanism: cloud data.

Cloud data is not stored locally, at least not all of it. Rather, the physical device contains tags, or permanent conduits (*i.e.*, saved encrypted passwords and account numbers) to data stored outside the physical device, on distributed systems shared across the internet. As one commentator summarized:

> Experts have coined the term 'Web 2.0' to describe the shift in Internet usage from consumption to participation and metaphorically refer to this virtual platform as 'the cloud,' where users interact with Internet applications and store data on distant servers rather than on their own hard drives.

David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2205 (2009).

Freed from physical restrictions, cloud computing allows cellphones to achieve infinite data capacity. By distributing data storage outside the device, and using the local storage to house conduits and tags to that data, pulling it down to the device on demand, there is literally nothing that cannot be stored on a device that fits in one's pocket.

B. Mobile Devices Have Been Incorporated Into Modern Living In A Fundamentally Private And Personal Way.

The mobile computing revolution has shifted societal concepts of identity and privacy in ways unimaginable just two decades ago. This Court has viewed the home as the epicenter of Fourth Amendment privacy. *United States v. U.S. Dist. Ct. E.D. Mich., S. Div.*, 407 U.S. 297, 313 (1972). Yet the Amendment on its face offers no distinction between "persons, houses, papers and effects."

At the time of the Fourth Amendment's enactment, the home was a locus of one's private life. Money might be held in a strongbox. Documents, deeds, wills, and investments would likely be stored in one's study. A diary detailing health problems and sickness might be tucked away in a drawer while personal letters and a family portrait would sit upon one's desk. In essence, the home was where the documentary evidence of one's self identity could be found. But the digital revolution has distributed those private pieces of one's life across cyberspace.

No longer is one's money tangible, and located in a strongbox, now it is accessible through a banking app. According to the Pew Research Center at least a

third of all mobile phone users regularly use the phone to manage their finances.[4]

A diary of one's ailments is no longer in a drawer, but is more likely to be in the cloud, accessible from a health application on a mobile phone. Over half of all smartphone owners use their phones to manage their health records, or to research health-related issues. Susannah Fox & Maeve Duggan, *Mobile Health 2012*, Pew Research Ctr. (2012).[5]

While paper correspondence has become a lost art, electronic correspondence has exploded. Ninety million Americans access email over a smartphone, and over 20 billion emails are accessed over smartphones each day worldwide. Radicati Grp., Inc., *Email Statistic Report, 2012-2016* (2012).[6] And although our mantles may still hold a small number of framed pictures, the real repository of our photographs exists on our phones and online. Facebook reports that users upload 350 million photographs to the site each day.[7]

---

[4] Report available at: Susannah Fox, *51% of U.S. Adults Bank Online*, Pew Research Ctr. (2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Online Banking.pdf.

[5] Report available at: http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf.

[6] Report available at: http://www.radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf.

[7] Report available at: Facebook, Ericsson & Qualcomm, *A Focus on Efficiency*, internet.org (2013), *available at* https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_520797877991079_393255490_n.pdf.

And 468 million users access those images daily on Facebook through a mobile application.[8]

Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living. Seventy-two percent of smartphone owners keep their phone within an arm's reach at all times. Jumio, *Mobile Consumer Habits 2013 Study*.[9] Sixty-five percent of all cellphone owners actually sleep with their phone. Amanda Lenhart, *Cellphones and American Adults* 11 (2010).[10] A 2012 survey found that 58% of phone owners check their phones at least once an hour, in bed before sleep and immediately upon waking. Harris Interactive, *Mobile Mindset Survey* (2012).[11] Over 50% use their phones while driving, nearly 20% use their phones during church, and 12% continue to use their phones in the shower. Jumio, *supra*.

The mobile computing revolution has created a virtual digital life that exists alongside and parallel to a physical life. Modern society now lives in both simultaneously, with each being integral to work, family, love, and daily living. And our mobile devices are the doorways to our virtual homes.

---

[8] Report available at: Josh Constine, *Facebook Reveals 78% of US Users are Mobile as it Starts Sharing User Counts by Country*, Tech Crunch (Aug. 13, 2013), http://techcrunch.com/2013/08/13/.

[9] Report available at: Jumio, *Mobile Consumer Habits 2013 Study* (2013), http://www.jumio.com/2013/07/americans-cant-put-down-their-smartphones-even-during-sex/.

[10] Report available at: http://pewinternet.org/~/media//Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf.

[11] Report available at: Harris Interactive, *Mobile Mindset Survey* (2012), *available at* https://www.lookout.com/resources/reports/mobile-mindset.

C. The Smartphone Is The New Instrument Of First Amendment Expression.

Lower courts have noted that, by their range of capabilities, ease of access, and societal saturation, smartphones are the quintessential free speech instruments of our age:

> The trial court aptly described a personal computer as 'the modern day repository of a man's records, reflections, and conversations.' CP at 200. Thus, the search of that computer has first amendment implications that may collide with fourth amendment concerns.

State v. Nordlund, 53 P.3d 520, 525 (Wash. Ct. App. 2002) (citation omitted). Even major news media such as the Chicago Sun Times have eschewed staff photographers, and now issue their reporters smartphones.[12]

This Court has afforded heightened protection to First Amendment instruments. The warrantless search of such material is a form of prior restraint, a long disfavored practice. *Roaden v. Kentucky*, 413 U.S. 496, 503 (1973) (When an officer "br[ings] to an abrupt halt an orderly and presumptively legitimate distribution or exhibition" of material protected by the First Amendment, such action is "plainly a form of prior restraint and is, in those circumstances, unreasonable under Fourth Amendment standards."). *See also Rossignol v. Voorhaar*, 316 F.3d 516, 522 (4th Cir. 2003) (Where sheriff's deputies suppressed newspapers critical of the sheriff "before the critical

---

[12] *See* Associated Press, *Chicago Sun-Times Lays Off All its Full-Time Photographers*, N.Y. Times (May 31, 2013), http://www.nytimes.com/2013/06/01/business/media/chicago-sun-times-lays-off-all-its-full-time-photographers.html?_r=3&.

commentary ever reached the eyes of readers, their conduct met the classic definition of a prior restraint.").

In an age when anyone can use a cellphone to blog, post to newsgroups, capture still images and video, send correspondence, and use all form of social mass communication, an officer's warrantless search of such a First Amendment instrumentality must be judged according to a stricter standard. *See Robinson v. Fetterman*, 378 F. Supp. 2d 534, 541 (E.D. Pa. 2005) (By restraining an individual from "publicizing or publishing what he ha[s] filmed," officers' "conduct clearly amount[s] to an unlawful prior restraint upon his protected speech."); *Channel 10, Inc. v. Gunnarson*, 337 F. Supp. 634, 637 (D. Minn. 1972) ("[I]t is clear to this court that the seizure and holding of the camera and undeveloped film was an unlawful 'prior restraint' whether or not the film was ever reviewed."). The warrantless seizure of material protected by the First Amendment "calls for a higher hurdle in the evaluation of reasonableness" under the Fourth Amendment. *Roaden*, 413 U.S. at 504.

This Court has noted that, when faced with a close call, "the First Amendment requires [courts] to err on the side of protecting . . . speech rather than suppressing it." *Fed. Election Comm'n v. Wis. Right to Life, Inc.,* 551 U.S. 449, 457 (2007); *see also Bertot v. Sch. Dist. No. 1, Albany Cnty., Wyo.,* 613 F.2d 245, 252 (10th Cir. 1979) ("We prefer that governmental officials acting in sensitive First Amendment areas err, when they do err, on the side of protecting those interests.").

II. The Warrantless Search Of A Smartphone Incident To Arrest Is Not Justified Under The Search Incident To Arrest Doctrine.

As this Court has consistently held, "the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment.'" *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971).

Exceptions to the warrant requirement are to be jealously and carefully drawn. *Jones v. United States*, 357 U.S. 493, 499 (1958). Such exceptions cannot be based upon mere governmental desire, or even need. Rather, warrant exceptions stake a claim to the Fourth Amendment's bedrock requirement of reasonableness only by "a showing by those who seek exemption from the constitutional mandate that the exigencies of the situation made that course imperative." *McDonald v. United States*, 335 U.S. 451, 456 (1948).

The search incident to arrest doctrine, as a historical exception to the warrant requirement, becomes reasonable only when two exigencies are present: "(1) the need to disarm the suspect in order to take him into custody, and (2) the need to preserve evidence for later use at trial." *Knowles v. Iowa*, 525 U.S. 113, 116 (1998) (citing cases going back to *Weeks v. United States*, 232 U.S. 383, 392 (1914)).

This Court laid down the "proper extent" of a seizure incident to lawful arrest in *California v. Chimel*, where it invalidated the search following respondent's arrest of his "entire three bedroom house, including the attic, the garage, and a small workshop." *California v. Chimel*, 395 U.S. 752, 754 (1969). Because "'[t]he scope of [a] search must be "strictly tied

to and justified by" the circumstances which rendered its initiation permissible,'" the *Chimel* Court set forth a rule to ensure that searches incident to arrest are linked to, and do not exceed, the two exigency rationales that render them "imperative." *Id.* at 761-62. Recognizing that weapons can be used to effect an assault or escape and evidence can be destroyed or concealed only to the extent they are accessible to the arrestee, this Court held that authorities, incident to lawful, custodial arrest, may search only an arrestee's person and his area of "immediate control . . . mean[ing] the area from within which he might gain possession of a weapon or destructible evidence." *Id.* at 763 (quotation marks omitted).

This Court's decision in *Robinson* did not alter the twin exigencies of *Chimel*. In *Robinson*, this Court held that:

> It is the fact of the lawful arrest which establishes the authority to search, and we hold 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.

United States v. Robinson, 414 U.S. 218, 235 (1973).

Robinson simply extended the need to establish officer safety and secure evidence to a defendant's pockets. *Robinson* never purported to countenance a general rummaging of one's life upon arrest, as this Court cautioned against in *Chimel*:

> After arresting a man in his house, to rummage at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant; indeed, the warrant would give

> more protection, for presumably it must be issued by a magistrate. True, by hypothesis the power would not exist, if the supposed offender were not found on the premises; but it is small consolation to know that one's papers are safe only so long as one is not at home.

395 U.S. at 767-68 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.))

The Supreme Court of California's decision in *People v. Diaz*, which controlled the outcome in this case, untethers *Robinson* from the *Chimel* rationale, rendering the result absurd. *People v. Diaz*, 244 P.3d 501, 505 (Cal. 2011). *Chimel* prevents a rummaging through one's home, but apparently under the government's interpretation, if technology advances sufficiently to digitize and shrink the contents of that home into one's pocket, the search becomes reasonable. The Constitution is not quantum mechanics; the rules do not break down when we move from the scale of the large to the small. *Chimel* still applies, and under *Chimel* the search is not permitted.

A. Neither Of The *Chimel* Rationales Is Present With Respect To The Warrantless Search Of A Cellphone.

Neither of the *Chimel* rationales supports the warrantless search of a cellphone incident to arrest. First, there is no officer safety concern posed by the data. Digital data is not a razor blade, or a firearm. It cannot harm, or in any way endanger, the arresting officers.

And once the phone is reduced to police custody, there is no reasonable likelihood of the destruction of evidence. Once the phone is in police control, the data is secure, just as the footlocker was secure in *United*

States v. Chadwick, where this Court struck down a search occurring 90 minutes after arrest. This Court reasoned that a search is not "incident to th[e] arrest either if the search is remote in time or place from the arrest or no exigency exists" and that authorities had removed the footlocker to "their exclusive control" before searching it, so "there [was] no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence." *United States v. Chadwick*, 433 U.S. 1, 15 (1977).

This Court reiterated the *Chimel*/*Chadwick* line of reasoning again in *Gant*, holding that the search incident to arrest of a vehicle already reduced to exclusive police control is not reasonable:

> In *Chimel,* we held that a search incident to arrest may only include 'the arrestee's person and the area 'within his immediate control' – construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.' *Ibid.* That limitation, which continues to define the boundaries of the exception, ensures that the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy . . . 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.

Arizona v. Gant, 556 U.S. 332, 339 (2009) (quoting *Chimel*, 395 U.S. at 763).

Respondent may argue, as does the Solicitor General in *United States v. Wurie*, that law enforcement

risks the data being "wiped" remotely. Pet'r's Br. 37-39, *United States v. Wurie*, No. 13-212 (U.S. Mar. 3, 2014). But that argument rings hollow. At the outset, this Court should note that the government offers no concrete example of that risk materializing. As Justice Scalia noted in the context of vehicle searches "the government . . . failed to provide a single instance in which a formerly restrained arrestee escaped to retrieve a weapon from his own vehicle." *Gant*, 556 U.S. at 352 (Scalia, J., concurring). The same holds true here. If remote data loss is a real threat to evidence the government should be able to provide this Court examples of cases in which data was lost during the time between seizure of a phone and the "hours or minutes necessary to obtain a warrant." *Chadwick*, 433 U.S. at 13.

Even if such case examples do exist, the objectively reasonable likelihood of data loss must be evaluated in reference to "the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59 (1968). It would be a rare case indeed, one involving a well-coordinated conspiracy of highly technically sophisticated suspects, where a threat of data wiping is even plausibly objectively reasonable. It certainly is not reasonable in respect to the vast majority of arrests for crimes such as DUI, assault, burglary, et cetera.

Moreover, in those very unusual cases where data wiping could even potentially occur, law enforcement has multiple ways to prevent the possibility from materializing.

First, law enforcement agencies throughout the country already employ portable devices, such as the CelleBrite UFED, designed to copy the entire data contents of a cellphone within minutes in the field.

Law enforcement proponents have praised the ease of use of the UFED device:

> Operation of the UFED is very straightforward. The investigator first needs to know the brand and model of the phone to be examined. More than 1,800 models are supported, and the list is updated at least once per month. Checking an index of supported models will indicate the data cable the investigator needs to use from the 80 supplied with the device. Connect the phone to the UFED using the appropriate cable (it's also possible to get the data via Bluetooth or IR port with some phones, but the data cable is the preferred method), tell the UFED what model phone it's examining, check the boxes alongside the types of information (phonebook, text messages, dialed numbers, photos, videos, etc.) to be retrieved, and press 'OK.'
>
> The entire process takes only a few minutes.

Tim Dees, *Roadside Cellphone Data Extraction* (2011).[13]

Second, law enforcement can employ a Faraday bag to shield a phone from data signals. This simple zip lock-style bag is made from the same material that prevents microwave ovens from spilling radiation into a kitchen. Shielded bags are widely available to law enforcement and the general public, and may be obtained from major retailers like Amazon at a minimal price point. *See, e.g.,* Dep't of Justice, Computer Crime & Intellectual Prop. Sec., *Awareness Brief: Find My iPhone* (June 18, 2009).

---

[13] Article available at: http://www.policeone.com/police-products/police-technology/mobile-data/articles/3592671-Roadside-cell-phone-data-extraction/.

Finally, if law enforcement is concerned about remote data wiping, it can employ the entirely effective and cost free solution of simply powering the phone off.[14]

III. Permitting A Warrantless Search Of A Smartphone, But Limiting It To Evidence Relating To The Crime Of Arrest Is Unworkable.

In *Gant*, this Court permitted the search incident to arrest of a vehicle when "it is reasonable to believe the vehicle contains evidence of the offense of arrest." *Gant*, 556 U.S. at 351. Echoing the Solicitor General's argument in *United States v. Wurie*, Respondent may ask this Court to graft that vehicle-specific rule onto the context of cellphones. *See* Pet'r's Br. 46-48, *Wurie*, No. 13-212. This Court should decline the invitation.

First, although the government may offer *Gant* as a practical limitation, in fact it is no limit at all in this context. Because of the quantity and scope of private information available on modern cellphones, and the myriad of ways we use those phones throughout our lives, an officer justifying a search after the fact in a suppression hearing will virtually always be able to draw a plausible connection between the crime and the data.

Take for example the routine DUI stop – a crime typically not requiring evidence beyond the observation of driving and a breath or blood test. Law en-

---

[14] Amici note that all of these options are themselves seizures of the phone and its data. And those seizures themselves carry constitutional implications. Amici's suggestion that UFED may obviate the need for a warrantless search should not be read as an endorsement that data copying by law enforcement is always a constitutionally permissible seizure of data.

forcement could theorize that a phone could contain pictures of the suspect drinking at the bar, text messages containing admissions of intoxication, digital receipts for the drinks ordered, and health records showing that the subject was on medication that interacted with alcohol.

A person texting while driving would have a connection between an arrestable traffic offense and their phone. Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 Ariz. L. Rev. 577, 579-80 (2012).

Low level possession of marijuana would support a phone search because the officer would only have to testify that many drug purchases are facilitated by text message. Similarly, every prostitution arrest would support the search of a phone, because perhaps the prostitute and patron coordinated via text message.

Indeed it is difficult to imagine a crime with respect to which law enforcement will not be able to say that in the officer's training and experience people tend to document their activities and leave digital records. The officer will only need to speculate about texts to potential undiscovered co-conspirators, possible photos showing the suspect with contraband, a GPS location near a crime scene, or web search history showing criminal planning to connect the phone to the crime of arrest and leverage that connection into a search of the data.

Further, the practical application of such a rule in the field is impossible. It is easy to define the acceptable parameters of a vehicle search. Objects can reasonably be located in certain places, and not in others. One need not look in the glovebox for a stolen

television. But how is an officer in the field supposed to know where in the phone to search for only the data connected to the crime of arrest?

Looking just to the online Apple application store, there are over one million unique applications available for mobile phone users, and over 1,000 new applications are added every day.[15] Existing applications are continually updated and modified, with new versions continually changing the interface and capabilities of the app. Many of the apps for mobile phones serve multiple purposes, making the type of data the app would hold difficult to determine. Applications like Snapchat mix photography with messaging. Applications like Health4Me combine messaging features with calendar appointment tracking and access to private prescription information.

This problem is further compounded by the fact that data is not cleanly divided into local data contained solely on the phone itself, versus distributed data located in the cloud. One cannot easily determine from an application where the data resides. And many applications blend local and cloud data in constructing what is displayed to the cellphone user.

The complexity and continually evolving nature of mobile data does not lend itself to ad hoc determinations made by individual law enforcement officers in the field. A *Gant* rule, or a rule that data located on the phone is searchable but distributed data is not, cannot be practically applied. *See* Pet'r's Br. 43-44, *Wurie*, No. 13-212 (arguing that a warrantless search is permissible as to local data, but conceding that such a search is impermissible as to distributed data).

---

[15] Statistics available at: *App Store Metrics*, 148 Apps, http://148apps.biz/app-store-metrics/ (last updated Mar. 3, 2014).

Imparting such rules to the cellphone context would mean requiring law enforcement officers in the field to know how each of those applications is used, which are financial applications, which hold photographs versus text, which might link to external data on the cloud, et cetera.

It would force law enforcement agents to become technology experts, knowing the latest models of devices and applications. And it would require law enforcement to become "technology sociologists," knowledgeable in the ways consumers are using the latest apps, how apps might disguise themselves as something else, or be renamed.

In short, *Gant* and other ad hoc solutions are not viable alternatives to unfettered searches in this context. The rule would simply amount to a *de facto* ratification of an exploratory search of the intimate details of an arrestee's digital life incident to arrest for any crime. It would be entirely unworkable in the field – save as a license to conduct broad and general searches of materials for which expectations of privacy are at their height. And finally, it would result in voluminous litigation. In nearly every case involving a cellphone search the defendant would demand a hearing on the officer's reasonable belief, what specific apps were searched, how the search was conducted, and how the officer chose certain data files over others. In many cases, expert testimony might be required to adequately assess the officer's explanation, and "battles of the experts" could proliferate.

IV. Cellphone Data Necessitates The Protections Of The Warrant Requirement.

The touchstone of the Fourth Amendment has always been reasonableness:

> The test of reasonableness under the Fourth

> Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted.

Bell v. Wolfish, 441 U.S. 520, 559 (1979).

The Fourth Amendment prefers warrants because warrants guarantee detached objective reasonableness in ways that warrant exceptions cannot. As this Court has said:

> '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. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. . . . 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.'

Coolidge, 403 U.S. at 449-50.

A. Technology Has Removed Impediments To Securing A Warrant.

As this Court has noted recently, advances in technology have significantly improved the ease and speed with which law enforcement can secure a warrant. *Missouri v. McNeely*, 133 S. Ct. 1552, 1562, (2013). Applications for warrants via telephone or email are permitted under the Federal Rules of Criminal Procedure, as well as the vast majority of states.

While the time to obtain a warrant is situation-specific, courts routinely report telephonic or email warrants being secured within minutes, or the length of a typical traffic stop. *See, e.g., Smith v. State*, 981 N.E.2d 1262, 1273 (Ind. Ct. App. 2013), *transfer denied*, 996 N.E.2d 328 (Ind. 2013) (warrant obtained during traffic stop); *State v. Zeller*, 172 Wash. App. 1008 (2012) (same); *State v. Hathaway*, No. A-3986-12T4, 2013 WL 6223364 (N.J. Super. Ct. App. Div. Dec. 2, 2013) (warrant obtained in 30 minutes).

B. A Warrant Is The Only Effective Mechanism For Managing Governmental Collection Of Cellphone Data.

This case is but one example of a widespread phenomenon. Law enforcement nationwide is systematically capturing, copying, and keeping vast amounts of data from arrestees all without a warrant.

In this case, the San Diego Police Department "downloaded" videos "along with a bunch of photos" from Riley's cellphone "through RCFL." J.A. 14. "RCFL" appears to refer to San Diego's Regional Computer Forensics Laboratory, established by the FBI in partnership with local law enforcement agencies in 1999. FBI, Dep't of Justice, *Regional Computer Forensics Laboratory Program: Annual Report* 46 (2012). The FBI now operates similar partnerships

with law enforcement in nineteen states, providing local officers with assistance duplicating, storing and preserving digital evidence. The FBI provides local police with access to "Cell Phone Investigative Kiosks," which allow officers to "extract data from a cell phone, put it into a report, and burn the report to a CD or DVD in as little as 30 minutes." *Cell Phone Investigative Kiosks*, RCFL, http://www.rcfl.gov/DSP_P_CellKiosk.cfm (last visited Mar. 3, 2014). In 2012 alone, the San Diego Police Department and other law enforcement agencies in the area used the kiosks 1,575 times to extract, copy, and retain cellphone evidence. FBI, *supra*, at 46. The kiosks are becoming increasingly popular with law enforcement nationwide. In 2012, law enforcement used the kiosks 8,795 times, a 48% increase from 2011. *Id.* at 6.

A predictable consequence of warrantless cellphone searches is that at least some of the information will eventually wind up stored in a government database. If police officers do not need a warrant to search a cellphone incident to arrest – if a personal electronic device is a mere "closed container" subject to full inspection – then police will surely claim the authority to conduct an unlimited search and use the information in any way they see fit. *See* Pet'r's Br. 12-13, *Wurie*, No. 13-212 (government arguing that *"any* warrantless search of items found on the person of an arrestee" is a "reasonable search" under *Robinson*, 414 U.S. 218 (emphasis added)); *United States v. Finley*, 477 F.3d 250, 260 (5th Cir. 2007) (determining that a cellphone is a "closed container" and therefore subject to a full search incident to arrest without any additional justification); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (permitting police to search the memory of pager incident to arrest under the "closed container" rule); *United States v. Chan*,

830 F. Supp. 531, 535 (N.D. Cal. 1993) (same). Absent a warrant requirement, police may consider themselves free to create a "mirror" copy of the data, retain it on a law enforcement database for detailed analysis, and share it with other law enforcement agencies as a matter of routine.

This is not idle speculation. Although the San Diego Police Department does not publish its procedures for handling digital evidence, the FBI's rules provide a glimpse into how law enforcement retains and shares electronic data belonging to thousands of Americans. At present, all telephone data collected during FBI investigations – including data extracted from cellphones seized incident to arrest – is stored in the FBI's Telephone Applications Database. That information feeds into the Investigative Data Warehouse (IDW), a central repository completed in 2005 for criminal and counterterrorism purposes. Office of Inspector Gen., Dep't of Justice, Audit Rep. No. 05-07, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project* (2005); Elec. Frontier Found., *Report on the Investigative Data Warehouse* § II (2009). At least 12,000 federal, state and local law enforcement and government officials have access to the IDW database. Office of Inspector Gen., Dep't of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 30 n.64 (2007). There are few limits on how long the FBI can keep data in the IDW. Bureau policy states that the data is deleted or destroyed only "when superseded by updated information or when no longer needed for analytical purposes." Office of Dir. of Nat'l Intelligence, N1-65-10-31, *Request for Records Disposition Authority* (2010).

Similarly, customs officials assert broad latitude to search and copy electronic devices at the border with-

out suspicion of criminal activity. U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* 3 (2009).[16] Officials routinely copy the contents of cellphones, cameras, and computers without any suspicion of criminal activity and keep the data if required for any "law enforcement purpose." *Id.* at 3. The Department of Homeland Security (DHS) then retains this information on a variety of databases for 5, 15, or 20 years, and may use or share it broadly to assist in national security and intelligence activities. Levinson-Waldman, *supra*, 37, 72 nn.320-21.

Such open-ended policies raise troubling questions about the constitutionality of copying, retaining, and sharing cellphone data without limit. Can police seize every bit of data on a phone, or only the relevant data? Will the plain view doctrine apply? How long can law enforcement keep the data it copies? Should there be a requirement to purge irrelevant information? Who else can see the data and for what purpose? Can the Internal Revenue Service take a look? The lack of appropriate safeguards creates a temptation to use the data for improper reasons. For example, the FBI's Office of Professional Responsibility recently reported that FBI employees had conducted more than 1,500 unauthorized searches on FBI and government databases to look up friends working as exotic dancers and celebrities they "thought were hot." Office of Prof'l Responsibility, FBI, *OPR's Quarterly All Employee E-mail January 2011 Edition*, at § 9 (Washington, D.C. Jan. 2011); Office of Prof'l Responsibility, FBI, *Quarterly Emails: #9 – April 2008*,

---

[16] Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

at § 14 (Washington, D.C. Apr. 2008).[17] A warrant requirement will not make these questions disappear, but it will ensure that troves of highly personal data do not wind up on a government computer network without adequate justification. Courts can craft reasonable parameters for the search that are consistent with the particularity requirement of the Fourth Amendment, minimize the invasion of privacy, and prevent personal data from being copied needlessly, kept indefinitely, or used improperly.

A bright line warrant requirement will also alleviate uncertainty for police officers in the field, placing questions regarding the scope of the search under *ex ante* judicial supervision. There may be a temptation to craft a graduated approach to cellphone searches; to require a warrant for copying the contents, but not to browse through a few screens, for example. But such an approach would force law enforcement officers with "only limited time and expertise" and in the heat of an investigation to "reflect on and balance the social and individual interests in the specific circumstances they confront." *Dunaway v. New York,* 442 U.S. 200, 214 (1979); *United States v. Wurie,* 728 F.3d 1, 6 (1st Cir. 2013), *cert. granted*, No. 13-212 (U.S. Jan. 17, 2014).

Absent a warrant requirement, there is simply no clear way to regulate the scope of the intrusion. Even the most cursory search – for example, a search for a particular name or number – can transform into an extensive forensic search that yields large volumes of private and sensitive information. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 565-66, 569 (2005). Moreover, there

---

[17] Available at: http://i2.cdn.turner.com/cnn/2011/images/01/27/fbi.documents.siu.pdf.

would be no mechanism to regulate how long police can keep cellphone data or control who has access to it. This Court has recognized that even an initially permissible seizure can become unreasonable "if it is prolonged beyond the time reasonably required to complete th[e] mission." *Illinois v. Caballes*, 543 U.S. 405, 407 (2005). But if there is no "mission" – if the only justification for seizing and searching cellphone data is that it occurs incident to arrest – then the scope of the intrusion is limited only by the officers' time and imagination. *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1171 (9th Cir. 2010) (observing that without judicially imposed limits on the scope of digital searches, "government agents ultimately decide how much to actually take . . . creat[ing] a powerful incentive for them to seize more rather than less"); Kerr, *supra*, at 544. Every police department in the country could have a different rule about what data to keep and share.

A neutral and detached magistrate is well placed to weigh the Fourth Amendment considerations in the balance and ensure meaningful limits on the scope of cellphone searches. *Comprehensive Drug Testing*, 621 F.3d at 1179 (Kozinski, J., concurring) (observing that magistrate judges can require the government to waive reliance on the plain view doctrine, segregate relevant evidence from unrelated data and return or destroy unrelated data). In some instances, there may be good reason to copy phone data or to conduct a forensic analysis, but that reason should be presented to a court before the government can "seize the haystack to look for the needle." *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).

CONCLUSION

For the foregoing reasons, amici urge this Court to reverse the decision of the California Supreme Court and hold that the search incident to arrest doctrine does not justify the search of the data contents of a cellphone.

Respectfully submitted,

JEFFREY T. GREEN
CO-CHAIR, AMICUS COMMITTEE
NAT'L ASS'N OF CRIMINAL DEFENSE LAWYERS
1501 K Street, N.W.
Washington, D.C. 20005

BRONSON D. JAMES*
BRONSON JAMES LLC
522 N.W. 23rd Ave.
Portland, OR 97210
(503) 943-6876
bj@bronsonjames.com

MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
161 Ave. of the Americas,
New York, NY 10013

Counsel for Amici Curiae

* Counsel of Record

March 10, 2014