No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondents.

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

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY-FOUR TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
GINGER MCCALL
ALAN BUTLER
DAVID HUSBAND
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

March 10, 2014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC)[1] is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts concerning privacy issues, new technologies, and constitutional interests: *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (No. 11-817); *United States v. Jones*, 132 S. Ct. 945 (2012); *Herring v. United States,* 555 U.S. 135 (2009); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada, Humboldt County,* 542 U.S. 177 (2004); *State v. Earls*, 214 N.J. 564 (2013); *Commonwealth v. Connolly*, 454 Mass. 808 (2009).

EPIC has an interest in upholding Fourth Amendment protections against unreasonable searches and seizures. In particular, EPIC is focused on preventing the erosion of constitutional privacy rights due to the emergence of new technologies. Cell phone privacy is of critical concern to all Americans,

---

[1] Both parties have filed letters of consent consent to the filing of all amicus briefs with the Clerk of the Court pursuant to Rule 37.3. 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.

as sensitive private data is now routinely stored and accessed via Internet-enabled smartphones.

Technical Experts and Legal Scholars

James Bamford, Author and Journalist

Colin J. Bennett, Professor, University of Victoria

Christine L. Borgman, Professor & Presidential Chair in Information Studies, UCLA

Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law

Simon Davies, Project Director, London School of Economics

Laura K. Donohue, Professor of Law, Director of The Center for National Security and the Law, Georgetown University Law Center

David Farber, Distinguished Career Professor of Computer Science and Public Policy, School of Computer Science, Carnegie Mellon University

Dr. Addison Fischer, Former Owner, RSA Data Security, Co-Founder, Verisign

Hon. David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Deborah Hurley, Chair, EPIC Board of Directors

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Ripple Labs Inc.

Harry Lewis, Gordon McKay Professor of Computer Science, School of Engineering and Applied Science, Harvard University

Anna Lysyanskaya, Professor of Computer Science, Brown University

Alice E. Marwick, Ph.D., Assistant Professor, Department of Communication and Media Studies, Fordham University

Mary Minow, Library Law Consultant

Dr. Pablo Molina, Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, SRI International

Ray Ozzie, (former) Chief Software Architect, Microsoft

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Eugene H. Spafford, Ph.D., D. SC., Professor, Purdue University

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Modern cell phone technology provides access to an extraordinary amount of personal data. Cell phone users routinely store sensitive and intimate information on a device that they keep close to their body. Misplacing a cellphone is an immediate cause for concern. Allowing police officers to search a

person's cell phone without a warrant following an arrest would be a substantial infringement on privacy, is unnecessary, and unreasonable under the Fourth Amendment. First, the warrantless search of a cell phone provides access to personal information and private files, stored both on the phone and on remote servers that are accessible from the phone. Second, there is no need to allow warrantless searches when currently available techniques allow law enforcement to secure the cell phone data pending a judicial determination of probable cause. Neither of the interests recognized by this Court underlying the search incident to arrest exception would justify the warrantless search of an individual's cell phone.

ARGUMENT

This case involves the warrantless search of Defendant's cell phone subsequent to his arrest. As this Court has repeatedly emphasized, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). This rule is subject to a few narrow exceptions, including certain searches incident to a lawful arrest. *Id.* However, no such exception justifies searching the vast array of information accessible from a cell phone without first establishing probable cause.

The search incident to arrest exception, outlined by the Court in *Chimel v. California*, 395 U.S. 752 (1969), and *United States v. Robinson*, 414

U.S. 218 (1973), is grounded in two interests: (1) the need to ensure officer safety and (2) the need to prevent the destruction of evidence. *Chimel*, 395 U.S. at 762-63. Searching a cell phone following an arrest serves neither of those interests.

In fact, modern cell phones provide access to so much information that a warrantless search would give the police unbridled access to that person's most sensitive information. Not only is the information on the device personal, users typically store account names, passwords, and other links to private data stored on remote computers. From a cellphone, users can even see into their homes and control devices and appliances.

Furthermore, the state's interest in obtaining evidence from the cell phone can be preserved without sacrificing Constitutional safeguards with simple and inexpensive security techniques. Best practices already recommend storing confiscated phones in packages, referred to as "Faraday bags," that block radio signals to prevent remote tampering. These simple and inexpensive procedures should be used to protect the phone and would give officers opportunity to obtain a judicial warrant to search the device if necessary.

The Fourth Amendment requires that officers obtain a warrant prior to conducting a search absent exigent circumstances. No special circumstances justify an exception to cell phones confiscated during a lawful arrest.

I. U.S. Consumers Are Dependent on Modern Cell Phones for a Wide Range of Personal and Business Activity

Cell phones are ubiquitous in the United States. More than 91% of American adults own a cell phone, Maeve Duggan, *Cell Phone Activities 2013*, PewResearch Internet Project (Sept. 19, 2013),[2] and wireless penetration – the number of active units divided by the total population – is over 100%. Fed. Commc'ns. Comm'n, *Mobile Wireless Competition Report (16th Annual)* 10 (Mar. 21, 2013).[3] The majority of phones are now sophisticated portable computers that provide constant Internet connectivity and a single point of access to all of the user's personal files, communications, and records. Phones are even expanding in size and functionality, and are now nearly equivalent to tablet computers. *See* Molly Wood, *Phone, Meet the Tablet.*, N.Y. Times, Feb. 27, 2014, at B8.

Cell phones are no longer simple communications devices used to send and receive calls, untethered from a wire. A majority of Americans now use Internet-enabled "smartphones" to send messages, surf the web, share photos, exchange files, get directions, use apps, and listen to music.[4] According to a recent poll, "Fully 68% of

---

[2] http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

[3] *Available at* http://www.fcc.gov/reports/mobile-wireless-competition-report-16th-annual.

[4] According to AT&T, a smartphone is:

adults connect to the internet with mobile devices like smartphones and tablet computers." Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PewResearch Internet Project (Feb. 27, 2014).[5]

Cell phones are also an increasingly important part of Americans' daily lives. As of June 2013, 56% of American adults use a smartphone. Aaron Smith, *Smartphone Ownership 2013*, PewResearch Internet Project (June 5, 2013).[6] Americans no longer use their phones solely for calling each other but also to browse online. PewResearch found that 63% of adult cell phone users use their phones to go online and

---

> a general term that refers to a cellular telephone that is more advanced than a feature phone. In general, a smartphone has an operating system that allows a user to do many of the things that were once reserved for a personal computer such as accessing the Web at higher speeds, viewing/editing documents, downloading files, creating music playlists, or managing multiple email/messaging accounts. Smartphones have advanced functionality, in addition to the standard functionality offered on a feature phone, such as the ability to send and receive text messages.

AT&T, *What is a Smartphone?* (2014), http://www.att.com/esupport/article.jsp?sid=KB101001&cv=821#fbid=m31wBrRSjwr.

[5] http://www.pewinternet.org/2014/02/27/summary-of-findings-3/.

[6] http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/

34% of these users go online mostly using their phones. *Id*. Americans use cell phones to send text messages (81%), access the Internet (60%), send or receive email (52%), download applications (50%), to get directions or location-based information (49%), to listen to music (48%), or to participate in a video call or video chat (21%). Maeve Duggan, *Cell Phone Activities 2013*, PewResearch Internet Project (Sept. 19, 2013).[7]

According to one industry report, 2013 was the first year that more than half of consumers (54%) no longer access the Internet from a single device (a desktop computer or a phone). The majority of Americans are now "multi-platform" users, meaning they browse the Internet from a combination of phones, computers, tablets, and other devices. This transition has been driven by the rising use of mobile applications ("apps"), with more than 85% of overall time on mobile phones spent within apps. Eli Goodman, *The Multi-Platform Majority: How Mobile is Changing the Way We Experience the Web*, comScore Blog (Dec. 9, 2013).[8] Mobile phones are already recognized as important tools with a wide range of educational, professional, and social uses. *See* Aaron Smith, *The Best (and Worst) of Mobile*

---

[7] http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

[8] http://www.comscore.com/Insights/Blog/The_Multi-Platform_Majority_How_Mobile_is_Changing_the_Way_We_Experience_the_Web.

Connectivity, PewResearch Internet Project (Nov. 30, 2013).[9]

Consumers now use many different mobile apps on their cell phones to access personal data. The average smartphone user in 2013 had thirty-three mobile apps installed, and "actively" used twelve different apps during each thirty-day period. ThinkInsights, *Our Mobile Planet*.[10] A full 75% of smartphone users access the Internet via apps every day. *Id*.[11] Consumers prefer to access the Internet via apps, which account for "4 out of every 5 mobile minutes, rather than the mobile web." ComScore, *2013 Mobile Future in Focus* (Feb. 22, 2013).[12]

The market for applications is accelerating, according to *The Growing App Market* (2012).[13] The study notes that 47% of the U.S. population has downloaded at least one app, 24% have paid for an app and that among users with phones that can

---

[9] http://www.pewinternet.org/2012/11/30/the-best-and-worst-of-mobile-connectivity/.

[10] Graphs available for the United States and other countries at http://think.withgoogle.com/mobileplanet/en/. See relevant data under "Key Activities" -> "Apps" -> "Number of Apps on Smartphone."

[11] See relevant data under "Mobile Internet Usage" -> "Frequency Mobile Internet Usage via Apps" -> "Daily."

[12] *Available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Mobile_Future_in_Focus

[13] *Available at* http://appdevelopersalliance.org/files/pages/The%20Growing%20App%20Market%20Slides%209-17-2012.pdf.

utilize apps, a full 74% of those users have downloaded an app. These apps enable cell phone users to access a variety of sensitive personal information stored either on the phone or remote Internet servers easily and seamlessly at any time.

In brief, the modern cell phone provides access to the single greatest concentration of personal information that could be conceived. For many users, their entire lives are accessible from their phones.

II. Modern Communications Providers Store Sensitive Personal Information on Remote Servers, Accessible to Authorized Users with Cell Phones, Tablets, and Other Devices

A majority of cell phone users now own smartphones, equipped with mobile applications that connect, synchronize, and deliver data stored and processed on remote servers. Many of these mobile "apps" allow users to access content across multiple platforms – on their phones, computers, and tablets. Modern phones not only provide access to files, messages, photos, and music, they also act as the keys that unlock a users' online identities. These devices provide access to remote repositories that contain private financial, medical, and communications records.

A. Mobile Apps Integrate Local and Remote Data to Provide Users With Access to Their Files and Communications

The proliferation of Internet-enabled mobile phones has fueled the development of mobile apps. *See* Pei Zheng & Lionel Ni, *Smart Phones and Next*

Generation Mobile Computing 51 (2010). These programs, downloaded and installed on the cell phone, access, display, and synchronize content that is stored remotely. The new generation of mobile apps download so much data that smartphone adoption has caused a "bandwidth jam in the United States," and mobile companies such as AT&T and Verizon are lobbying for additional wireless spectrum to increase capacity. *Communication Technology Update and Fundamentals* 260 (August E. Grant & Jennifer H. Meadows eds., 2012).

Users access e-mail messages, calendars, photographs, files, notes, and other personal data on all their devices – phones, computers, and tablets – via mobile apps. For example, Apple's service:

> iCloud stores your music, photos, apps, mail contacts, calendars, documents, and more and wirelessly pushes them to all your devices. So if you buy a song, take a photo, or edit a calendar event on your iPad, iCloud makes sure it appears on your Mac, iPhone, and iTouch, too.

Apple, *What is iOS 7* (2014).[14] *See also* Zheng & Ni, *supra* at 52 ("*E-mail, calendar, organizer, and notepad* are typical PIM [personal information manager] applications. Web-based PIM services such as Yahoo! allow users to synchronize personal data, including e-mail, personal calendars, organizers, and address books, from the web to PDA's or cell phones")

[14] http://www.apple.com/ios/what-is/.

(emphasis added). The e-mail apps on Apple iOS[15] and Android,[16] the two most common mobile operating systems, are configured to download new messages whenever the user opens the app. Many users configure their phones to receive e-mail messages automatically whenever they are available. *See* Rob LeFebvre, *Fetch or Push? Set Your E-mail Accounts to Maximize Battery Life, Speed of Delivery*, Cult of Mac (Aug. 5, 2013).[17]

Many mobile apps display a mix of locally stored and remotely synchronized content on the user's device. When a user opens an app, "Content such as pictures or video is [downloaded] over the Internet via a mobile data connection ([or] Wi-Fi), and once the content is embedded in the device (your smartphone), the data connection can be closed and the content viewed offline (when you aren't connected to the Internet." Peggy Anne Salz & Jennifer Moranz, *The Everything Guide to Mobile Apps* 15 (2013).

These programs, widely used on cell phones today, rely on remote servers that continuously

---

[15] *See* Apple, *iPhone User Guide* 49 (2013), *available at* http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

[16] *See* Google, *Android Quick Start Guide* 36 (2013), *available at* http://static.googleusercontent.com/media/www.google.com/en/us/help/hc/images/android/android_ug_42/Android-Quick-Start-Guide.pdf.

[17] http://www.cultofmac.com/238746/fetch-or-push-set-your-email-accounts-to-maximize-battery-life-speed-of-delivery-ios-tips/.

transfer data back and forth between the devices and the servers. This model of computing is sometimes described as "cloud computing."[18] When a user views or searches their e-mail, photographs, financial records, or other sensitive information from a mobile apps, that data is downloaded from the server to the phone as it is presented to the user alongside previously downloaded data.

From the user's perspective, the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable. App data is continuously updated in order to ensure that the data is synchronized across all the users' devices. According to Deloitte, the rise in "converged, connected devices" leads to a situation where "consumers are increasingly storing and synchronizing files in the cloud," such that by the end of 2013, "there will be some 600 million personal cloud subscriptions, and that number is expected to double by the end of 2017." Deloitte, *The State of the Global Mobile Consumer* 6 (2013).[19] In fact, many apps now provide updates even when the user does not have them open. *See* Apple, *iOS: Understanding Notifications* (2014).[20] By default, Apple devices allow

---

[18] For a brief description of cloud services, see Goodwill Community Foundation, *What is the Cloud?* (2014), http://www.gcflearnfree.org/computerbasics/extra/82.

[19] *Available at* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT-GMCS_January%202014.pdf.

[20] http://support.apple.com/kb/ht3576.

these notifications to be viewed even when the phone is locked. *Id.*

This cloud-based model attempts to ensure that the user will see the same messages, files, and records no matter where they are. The data "stored" on the phone might provide a momentary snapshot of the user's activities, but the phone will continue to download additional data from remote servers. Modern phones are constantly downloading, or "pulling" new data and remote servers are constantly sending, or "pushing," updates, including private messages, breaking news, and alerts.

B. Mobile Apps Provide Access to Sensitive Information on Remote Servers

The popularity of smartphones has lead to an explosion in mobile apps. For users of just one popular cell phone, there are now more than 1 million different apps available. *See* Chuck Jones, *Apple's App Store to Hit 1 Million Apps*, Forbes (Dec. 11, 2013);[21] AppBrain, *Number of Available Android Apps in the Market* (2014).[22] These programs enable users to access a variety of services and download up-

---

[21] *Available at* http://www.forbes.com/sites/chuckjones/2013/12/11/apples-app-store-about-to-hit-1-million-apps/. According to a popular Apple iOS development page, there are 1,135,438 active apps in the Apple store. *Apple Store Metrics*, http://148apps.biz/app-store-metrics/ (last visited Mar. 7, 2014).

[22] http://www.appbrain.com/stats/number-of-android-apps. There were 1,132,053 available Android apps as of February 13, 2014. *Id.*

to-date information. Many of these apps connect users with sensitive personal data that is stored on remote servers, including:

- E-mails and messages
- Calendars
- Notes
- Personal files
- Financial records, and
- Medical records

Some apps enable direct remote control of systems and devices within the users' homes.

Messaging Services

Mobile phone users rely on a variety of applications to send electronic communications. Email providers such as Google store older emails in the cloud. Google, *Gmail Help: Open & Read Email* (2014).[23] These messages can then be accessed by the user (or anyone in possession of the phone), by either scrolling down or conducting a keyword search. *Id*. The email provider then pulls the relevant messages

---

[23]https://support.google.com/mail/topic/2819493?hl=en&ref_topic=2772286. *See also* Google, *Getting Started with IMAP and POP3* (2014), https://support.google.com/mail/troubleshooter/1668960?hl=en (Google "encourage[s] you to use IMAP" because "IMAP offers two-way communication between your web Gmail and your email client. This means when you log into Gmail using a web browser, actions you perform on email clients and mobile devices . . . will instantly and automatically appear in Gmail").

from the cloud and makes them visible to the mobile phone user. *Id*.

Mobile phones also provide access to online social networking tools. Online social networking tools contain a variety of sensitive personal information, including information about users' associations and friendships, photographs, and communications.

Most social networks provide private messaging services in addition to public message posting. Facebook, the most popular social network service, with over 1.23 billion users worldwide and 945 million monthly mobile users, Facebook, *Key Facts* (2014),[24] allows users to add friends, communicate privately via either an instant messaging tool, an email-like messaging service, or both. Twitter, another popular social network, has over 645 million users, 43% of which use their phone to tweet. Statistic Brain, *Twitter Statistics* (Jan. 1, 2014).[25] Twitter users can publicly post text or picture messages – "tweets" – or can send private, "direct messages" to other users.

As of October 2013, Google's social network, Google+ had 540 million active users, including 300 million monthly users, who uploaded an average of 1.5 billion photos every week. Matt McGee, *Google+ Hits 300 Million Active Monthly "In-Stream" Users, 540 Million Across Google*, Marketing Land (Oct. 29,

---

[24] http://newsroom.fb.com/Key-Facts.

[25] http://www.statisticbrain.com/twitter-statistics/.

2013).[26] Google+ also allows users to make public posts, limited-audience posts, and to send private communications to other users.

These social networks are easily accessible on cell phones with mobile apps. These apps provide access to a user's account, including private communications, personal photographs, and contact lists. Facebook, Twitter, Google+ and Snapchat all have popular mobile apps. In fact, according to Adobe's 2013 Mobile Consumer Survey, accessing social media is "the number one mobile activity today. . . .Of those surveyed, 71% reported using their mobile device to access social media." Ray Pun, *Adobe 2013 Mobile Consumer Survey: 71% of People Use Mobile to Access Social Media*, Adobe Digital Marketing Blog (July 25, 2013).[27]

Photo and Video Sharing

Mobile phone applications also allow users to access and share photographs and videos. YouTube enables cell phone users to send private videos to other cell phone users. YouTube, *Video Privacy Settings* (2014).[28] These videos can include very personal user-created content. YouTube's application allows a user to access his or her playlists of videos,

---

[26] http://marketingland.com/google-hits-300-million-active-monthly-in-stream-users-540-million-across-google-63354.

[27] http://blogs.adobe.com/digitalmarketing/mobile/adobe-2013-mobile-consumer-survey-71-of-people-use-mobile-to-access-social-media/.

[28]https://support.google.com/youtube/answer/157177?hl=en

which are stored on the company's external servers. Google Play Store, *YouTube Application Page* (2014).[29]

Flickr is a photo hosting service that has similar features. The service allows users to upload photographs, which may be shared publicly or kept private. Yahoo!, *Privacy Policy: Flickr* (2014).[30] Users can "choose to make your photos default to public for anyone to access, restrict access to a limited number of other Flickr users, or keep those photos private so only you can access them." Like YouTube, Flickr has a mobile application that allows the user to access remotely stored photos, including photographs that have been designated as "private," on a mobile device. Google Play Store, *Flickr Application Page* (2014).[31]

Apple also has a built-in photo-sharing feature for iPhone users. *See* Apple, *iCloud Photo Sharing* (2014).[32] This app allows users to create and share photos with other users, and "each new addition is instantly broadcast to the photo stream of everyone in your group." *Id.* Users even get "real time notifications" of updates or new photos posted to their streams. *Id.* This means that at any time a users

---

[29]https://play.google.com/store/apps/details?id=com.google.android.youtube&hl=en.

[30] https://info.yahoo.com/privacy/us/yahoo/flickr/details.html.

[31] https://play.google.com/store/apps/details?id=com.yahoo.mobile.client.android.flickr.

[32] https://www.apple.com/icloud/icloud-photo-sharing.html.

phone could automatically receive new private photos from their friends, without even opening the app.

Personal Information Managers

There are many services, operating on cell phones, designed to assist in the management of personal information. For example, Evernote, promises, "all of your notes, web clips, files, and images are made available on every device and computer you use." Evernote, *Keep Everything in Sync* (2014).[33] Google provides a similar service with Google Sync, which encourages users to "Sync your Google services to your phone, tablet, and desktop programs, so that you can always access what's important to you." *See* Google, *Sync Your Mail, Contacts, Calendar, and More* (2014).[34] Other services enable businesses to managing their schedules and information remotely. For example, Full Slate includes an online scheduler, Calendar Sync, an appointment app for iPhone or Android, and a Client Database to "keep track of contact information, appointment history, and email correspondence in one place." Full Slate, *Client Database* (2013).[35]

All of these services enable access to detailed personal information directly from a cell phone.

---

[33] http://evernote.com/evernote/.

[34] http://www.google.com/sync/.

[35] https://www.fullslate.com/client-database.

Remote File Storage

File storage is one of the most popular cloud-based services. These services allow users to store, access, edit, and share their files, including word processing documents, presentations, spreadsheets, pictures, music, and videos. Some of the most popular file-storage services are Dropbox,[36] Apple's iCloud,[37] Amazon Cloud Drive,[38] Box,[39] Google Drive,[40] MediaFire,[41] and Windows Live OneDrive.[42]

Many of these file storage services can be accessed from mobile apps installed on a cell phone, allowing the user to access the information, even though the information is not itself stored on the phone. These files are private and can include a great deal of sensitive personal information – financial records, private messages, photographs, personal notes, and health records.

A person in possession of the cell phone therefore has access to this information even though it is stored on remote servers.

---

[36] *Dropbox*, https://www.dropbox.com/ (2014).

[37] *Apple iCloud*, https://www.apple.com/icloud/ (2014).

[38]Amazon, *Cloud Drive Photos for iOS* (2014), https://www.amazon.com/gp/feature.html/ref=cd_nav_ios?ie=UTF8&docId=1001206201.

[39] *Box*, https://www.box.com/ (2014).

[40] *Google Drive*, https://drive.google.com (2014).

[41] *Media Fire*, http://www.mediafire.com/ (2014).

[42] *Windows Live OneDrive*, https://onedrive.live.com/about/en-us/ (2014).

Financial Records

The entire world of personal finance is moving on to the cell phone. Mobile banking is "on the cusp of transformation from a niche service for the technologically elite to a mass-market service demanded by all customer segments." Deloitte Consulting, *Mobile Banking: A Catalyst for Improving Bank Performance* (2010).[43] At the time Deloitte noted that 10% of mobile users conduct some banking transactions via phone and that mobile banking usage increased at "nearly a 100% compounded annual growth rate" from 2005-2010, with most of the growth concentrated after 2007. *Id.*

The Federal Reserve recently described mobile banking as "using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone." Bd. of Gov's of the Fed. Reserve Sys., *Consumer and Mobile Financial Services 2013* (Mar. 2013).[44]

---

[43] *Available at* https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_consulting_MobileBanking_010711.pdf.

[44] *Available at* http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf (last visited Feb. 28, 2014).

According to the Federal Reserve, in 2013, 28% of all mobile phone users and 48% of smartphone users, have used mobile banking within the past twelve months. The most common use of mobile banking is to check account balances or recent transactions (87%). 15% of mobile phone users have made a mobile payment within the past twelve months, *Consumer and Mobile Financial Services 2013*, *supra* at 4, and 49% of mobile banking users utilize mobile apps to conduct their mobile banking transactions. *Id*. at 10.

The main reason more consumers do not use mobile banking is concern about security (38%). *Id*. at 14. The sensitivity of financial information underscores the privacy concerns that arise when this data is accessible from a phone.

Mobile apps also provide access to other financial data. For example, Mint is a popular financial tracking app that aggregates all of a user's financial accounts and records into one place. *What is Mint* (2014),[45] Many banks also have dedicated apps that provide their customers with mobile account access. *See*, *e.g.*, Bank of America, *Mobile Banking* (2014);[46] Wells Fargo, *Mobile App* (2014);[47] Chase, *Mobile App* (2013).[48] Thus, a user's current financial

---

[45] https://www.mint.com/what-is-mint/.

[46] https://www.bankofamerica.com/online-banking/mobile.go.

[47] https://www.wellsfargo.com/mobile/apps/.

[48] https://www.chase.com/content/chasecom/en/mobile-banking/mobileresponsive.

statements, stored on the bank's remote server, are easily accessible via an app on their phone.

Medical Records

Many users rely on their cell phones to access sensitive medical information, including records detailing medical conditions, exercise, nutrition, menstrual cycles, and medication use. According to Pew Research, 19% of smartphone users have a health app on their phone. Susannah Fox and Maeve Duggan, *Mobile Health 2012*, PewResearch Internet Project (Nov. 8, 2012).[49]

Some of these applications provide complete access to medical history files that would disclose sensitive information about health conditions and medications. The Medicare Blue Button allows patients to download their medical history into a simple text file on their smartphone. Elizabeth Stawicki, *Your Smartphone Might Hold Key to Your Medical Records,* Kaiser Health News (June 17, 2013).[50] Third party applications then help the user organize this information. Cloud-based document storage system Box provides a medical record storage system called "drchrono" that "is a medical platform for doctors and patients. The platform is divided into cloud based electronic health records, practice management, personal health records, and revenue

---

[49] http://www.pewinternet.org/2012/11/08/mobile-health-2012/.

[50]http://www.kaiserhealthnews.org/stories/2013/june/17/electronic-health-records-blue-button.aspx.

cycle management. The primary purpose of drchrono is to provide mobile healthcare through iPad, iPod touch, and iPhone." Box, *drchrono Description* (2014).[51]

Other applications allow users to log information about their fitness habits, *The Fitbit Story* (2014),[52] nutritional intake, *id*. ("Log your food with Fitbit's online tools and mobile apps to get a more complete view of your health and fitness."), menstrual cycles,[53] blood pressure,[54] and medication times.[55]

As with financial information accessible from a cell phone, users have expressed a clear desire for privacy regarding health data. Deloitte Consulting reports that 35% of survey respondents stated that they were concerned that the privacy and security of

---

[51] https://app.box.com/services/drchrono (last visited Feb. 28, 2014).

[52] http://www.fitbit.com/story ("Track everyday activity like steps, distance, calories, stairs climbed, and active minutes").

[53] Tamtris Web Services Inc., *Fertility Friend*, iTunes Preview (2014), https://itunes.apple.com/us/app/fertility-friend-ovulation/id443919067?mt=8.

[54] Taconic System LLC, *Blood Pressure Monitor*, iTunes Preview (2014), https://itunes.apple.com/us/app/blood-pressure-monitor-family/id430133691?mt=8.

[55] Medisafe Project, MediSafe Meds & Pill Reminder, Google Play Store (2014), https://play.google.com/store/apps/details?id=com.medisafe.android.client.

their personal information might be at risk when using a mobile device to access health records or tests online. Deloitte Consulting, *mHealth: a Check-up on Consumer Use* (2014).[56]

Remote Desktop Clients

Mobile apps even enable users to access their home computers remotely from their cell phone. From these "remote desktop" apps, users can view and control their desktop computers, including running programs, viewing files, and connecting to the remote network. *See* Citrix, *GoToMyPC: Remote Access Factsheet* (2013).[57]

This means that if a user has installed the software on their home or work computer, and configured the mobile app on their cell phone, anyone with access to the phone can "simply open the app," enter the user's credentials, and be "instantly connected to" that remote computer. Citrix, *GoToMyPC: Total Mobility – Factsheet* (2013).[58] These apps are especially popular with employers now because they can be used to "[i]ncrease employee productivity and flexibility." *Id*.

---

[56]http://www.deloitte.com/view/en_US/us/Insights/centers/center-for-health-solutions/5aa32defd7b21410VgnVCM2000003356f70aRCRD.htm.

[57] *Available at* http://l1.osdimg.com/remote-access/dam/pdf/white-papers/GoToMyPC_Factsheet.pdf.

[58] http://l1.osdimg.com/remote-access/dam/pdf/white-papers/GoToMyPC-Mobile-Remote-Access-Factsheet.pdf.

As a consequence, possession of a cell phone may provide access not only to files maintained by third party companies on the user's behalf but also to personal information stored directly on computers within the user's home.

Internet-enabled Home Appliances

Mobile phones now also provide for direct control of appliances and utilities in the user's home. Ninety-three percent of smartphone users recently expressed interest in using their mobile phones to remotely control their home temperature, lights, and other utilities. Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything* 9 (2014).[59]

For example, General Electric offers the GE Brillion App to control home appliances, such as ovens via your smartphone. General Electric, *GE Brillion Connected Appliances* (2014).[60] Currently, the GE Brillion App only works with GE Double Wall or Single Wall Ovens, but GE notes that "Coming in 2014, GE will expand its line of Brillion-enabled appliances." *Id.* Nest, recently acquired by Google, has devised the Nest Thermostat, which "can learn your schedule, programs itself, and can be controlled from your phone." Nest, *Life with Nest Thermostat* (2014).[61] Nest also makes a smoke alarm that can

---

[59] *Available at* http://www.wi-fi.org/system/files/wp_Wi-Fi_Internet_of_Things_Vision_20140110.pdf.

[60] http://www.geappliances.com/connected-home-smart-appliances/.

[61] https://nest.com/thermostat/life-with-nest-thermostat/.

send mobile alerts to your phone when an alarm sounds and whose features can be controlled from the mobile application. Nest, *Smoke Co-Alarm, Inside & Out* (2014).[62]

The Nest App, installed on a cell phone, can control both the Nest Thermostat and Smoke Alarm, which enables you to "change the current target temperature or view your energy usage on your Nest Thermostat, view the latest status, and adjust the settings on your Nest Protect, and much more." Nest, *Learn More about the Nest App* (2014).[63]

These mobile applications provide access to the inside of a home even when outside the home. The apps also give police officers who seize a cell phone access to data about the inside of the home and the possibility of affecting the internal temperature, turning on or off the gas furnace, and detecting historical variations in temperature. They provide information regarding the homeowner's schedule ("To save energy, Nest learns your schedule and preferences to program itself." Nest, *Saving Energy* (2014).[64] Possession of the cell phone could therefore provide intimate information to police about the activities of an individual within their home, without police ever obtaining a warrant to search the home.

---

[62] https://nest.com/smoke-co-alarm/inside-and-out/#teardown.

[63] http://support.nest.com/article/Learn-more-about-the-Nest-app.

[64] https://nest.com/thermostat/saving-energy/#we-didnt-think-thermostats-mattered-either.

C. Cell phones also operate much like a password, providing access to remote files and information that would not be available to an unauthenticated user

Mobile apps provide users with access to a wealth of private data, but they also provide an easy way to access and consolidate user's various online identities – social media accounts, bank accounts, e-mail accounts, and other profiles. Users are typically required to create unique, complex passwords for their various accounts. This can be a headache for many users. *See* Troy Hunt, *The Only Secure Password is the One You Can't Remember*, Lifehacker (Mar. 24, 2011);[65] Phillip Inglesant & M. Angela Sassse, *The True Cost of Unusable Password Polices: Password Use in the Wild*, Proc. SIGCHI Conf. Hum. Factors Comp. Sys. (2010) ("We find that users are in general concerned to maintain security, but that existing security policies are too inflexible to match their capabilities, and the tasks and contexts in which they operate.").[66]

But most mobile devices now solve this problem by storing passwords and other login information on the device so that the person in possession of the device is able to access all of the password-protected services. Apple now offers a similar service as part of its iPhone software. *See*

---

[65] http://lifehacker.com/5785420/the-only-secure-password-is-the-one-you-cant-remember.

[66] *Available at* http://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf.

Apple, *What is iOS* (2014) ("Most websites you visit nowadays require user names and passwords. Remembering them all can be tough. So let iCloud Keychain do it for you."). Some mobile apps also keep users logged in by default. Other apps provide storage of user login information for many sites and applications in one place. This means that a user's online identities are all easily accessible to anyone who has access to their phone.

Many applications have password saving features and generally, "by default, applications will store your passwords and never ask you for them again." Jonathan Garro, *Mac Computer Skills: Unlock the Power of Your Mac's Keychain Utility*, Tuts+ (April 15, 2013).[67] For example, when a user logs into Facebook via their cell phone, the app will keep the user logged in by default and store the password information. Some social media accounts, such as Twitter and Facebook, are even embedded into the phone software, requiring the user to take affirmative steps to log out. *See* Twitter, *How to Sign Out of Twitter for iPhone* (2014);[68] Facebook, *How do I log out of the iPhone or iPad App?* (2014).[69] This is a desired feature for many mobile phone users due to

---

[67] http://computers.tutsplus.com/tutorials/unlock-the-power-of-your-macs-keychain-utility--mac-48730.

[68] https://support.twitter.com/groups/54-mobile-apps/topics/222-ios/articles/20170805-how-to-sign-out-of-twitter-for-iphone#.

[69] https://www.facebook.com/help/iphone-app/112099682212213?rdrhc.

its convenience and is widely utilized. But it poses a serious privacy problem if law enforcement officers are allowed to access the user's phone without probable cause.

Users can also install a specific app, called a password manager, to store all of their online login information. Many of these password managers are available for current smartphones, including Last Pass, Onesafe, and 1Password. Kit Eaton, *Apps to Protect Your Array of Passwords,* N.Y. Times, Oct. 17, 2013, at B10. The user enters the passwords for all the websites and applications they wish to use, including banking, medical, and other extremely sensitive accounts they may have. These passwords are secured by a master password. The password manager then logs into the various other applications without the user needing to enter log in information. As with the in app storage of passwords, the data stored on the phone provides access to large amounts of data not stored on the phone.

In addition to storing passwords that provide access to a user's online identities, the smartphone can also be used to authenticate the user on other systems. This type of authentication, commonly referred to as "two-factor authentication," is offered by companies such as RSA (RSA SecureID Software Authenticators)[70] and Google (Google

---

[70] RSA, *RSA SecurID Authenticators: The Gold Standard in Two Factor Authentication* (2011). Available at: http://www.emc.com/collateral/data-sheet/h9061-sid-ds.pdf.

Authenticator).[71] Two-factor authentication requires that a user enter a unique numeric code, generated by a phone or other device, in addition their password to access the account. This prevents an unauthorized individual from accessing an account simply by knowing the password. In this way, cell phones act as a "key" to the user's online and offline identities.

Thus, a mobile phone acts as a master key that can grant access to, and prove a connection with, all of the user's various online and offline identities. The phone provides a portal to personal data stored on the cloud. Like a password, control over the phone is control over the data.

New apps can even replace physical keys and provide entry into a user's automobile or home. Bluetooth technology works with all vehicles and all Bluetooth enabled cell-phones, from a range of 5-15 feet, to unlock the user's car without a key. The product is designed so that "you can simply approach the vehicle which will unlock automatically. As you leave the parked vehicle, the module will also lock the vehicle." Bluetooth Keyless, *FAQs About the Bluetooth Passive Keyless Entry Module* (2014).[72] For customers who buy the Premium version of the product, the company provides an app customized to the individual phone's operating system such as iOS or Android. *Id.* An officer armed with this app could

---

[71] Google, *Google Authenticator* (2014), https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2.

[72] http://bluetoothkeyless.info/bluetooth-keyless-information/.

identify the user's car and even unlock it from nearby. Similar functionality exists for home entry. Lockitron, *Keyless Entry Using Your Phone* (2014).[73]

III. Law Enforcement Can Easily Mitigate the Risk of Cell Phone Data Loss Pending a Judicial Determination of Probable Cause

Cell phones may contain data, such as location data, text messages, and pictures, that may be useful as evidence to law enforcement,. Rizwan Ahmed, Dr. Rajiv V. Dharaskar, & Dr. Vilas M. Thakare, *Digital Evidence Extraction and Documentation From Mobile Devices*, 2 Int'l J. Advanced Res. Comp. & Comm'n Eng. 1019, 1022 (Jan. 2013). This data is stored in either the subscriber identity module (SIM) card, which contains information necessary for identifying the device on the cell network, Eoghan Casey & Benjamin Turnbull, *Digital Evidence on Mobile Devices*, in *Digital Evidence and Computer Crime* 5 (2011),[74] other external memory, such as an SD card which can be easily removed from the device, *id*. at 6, and the internal memory, which cannot be easily removed from the device. *Id.*

The standard for mobile devices, including laptops and cells phones, is to utilize a type of storage called flash memory. *Id.* at 3. Flash memory is non-volatile, meaning that the data will be retained even

---

[73] https://lockitron.com/.

[74] *Available at* http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

if the storage device is powered down. Russell Kay, *Flash Memory*, ComputerWorld (June 7, 2010).[75] Because flash memory only has a limited number of times data can be written on it, deleted data can remain for some time. Casey & Turnbull, *supra* at 3. This depends on the methods used to delete the data. Thorough sanitization of flash-based storage requires writing over the data multiple times, which lowers the life expectancy of the hardware. *See* Michal Wei et al., *Reliably Erasing Data From Flash-Based Solid State Drives*, 9th USENIX Conf. File & Storage Tech. (2011).[76]

A. Standard, Low-cost Security Techniques Enable Law Enforcement to Significantly Reduce the Risk of Cell Phone Data Loss

Some courts have expressed concern that cell phone data could be "remotely wiped" subsequent to a user's arrest. *See United States v. Flores-Lopez*, 670 F.3d 803, 807-808 (7th Cir. 2012). However, this concern can be easily mitigated with currently available security measures, and does not justify the warrantless of a confiscated device. Once the phone is secured, law enforcement officers can obtain a

---

[75] http://www.computerworld.com/s/article/349425/Flash_Memory.

[76] https://www.usenix.org/conference/fast11/reliably-erasing-data-flash-based-solid-state-drives (last visited Mar. 10, 2014).

warrant based on probable cause to search the phone if necessary.

There are three techniques that can preserve data on cell phones while a warrant is obtained: the use of data extraction devices, Faraday Bags, and aluminum foil. There is also the simple step of removing the battery from the device

Current best practices recommend that law enforcement officers turn off cell phones immediately upon confiscation. For example, the Drug Enforcement Administration guidance to law enforcement departments warns that officers "should be aware that when seizing a cell phone, the owner can remotely delete all personal data from the phone." El Paso Intelligence Center, *Tactical Intelligence Bulletin EB 11-09: Preserving Cell Phone Data* (2011).[77] The DEA recommends that the battery be immediately removed so that remote wiping signals cannot be received and that if the battery cannot be removed, the cell phone should either 1) be wrapped in aluminum foil or 2) be placed in a Faraday type box, which prevents the signal from being received. *Id.*

The Association of Chief Police Officers ("ACPO") in the United Kingdom has created a similar practice guide for handling electronic evidence, which includes a section entitled "Guide for Mobile Phone Seizure & Examination." Association of

---

77 https://www.ileas.org/sites/default/files/Preserving%20cell%20phone%20data.pdf.

Chief Police Officers, *Good Practice Guide for Computer-based Electronic Evidence* 48 (2008).[78] The ACPO Principles of Evidence provide basic guidance for police officers seizing evidence from electronic media. *Id.* at 4.[79] This ACPO advises officers when seizing a device to "Isolate the device from the network" and suggests officers: "Turn Device off at point of seizure," or "Place Device in shielded container/bag." *Id.* at 48. When examining the mobile

---

[78]http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[79] The Principles state:

> Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
>
> Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

phone, the ACPO recommends that a shielded room or container be used, but discourages the use of jamming devices, which are often illegal. *Id.*

The National Institute of Standards and Technology ("NIST") addressed this issue in a report on Cell Phone Forensics. Nat'l Inst. of Stds & Tech, *Guidelines on Cell Phone Forensics*, Special Pub. No. 800-101 (May 2007).[80] In this report, NIST applied the ACPO Principles of Evidence and emphasizes the need to "isolate the phone from other devices used for data synchronization" and reaffirmed that the basic methods to isolate the phone from a radio network are to turn the device off or to place it in a shielded bag. *Id.* at 33-34. NIST also stated that putting the phone in "Airplane Mode" is another alternative, but has the drawback of "requiring interaction with the phone via the keypad, which poses some risk." *Id.* at 34.

Faraday Bags

To block the radio network signal, one commonly used tool is a Faraday bag. These are "specially designed RF [radio frequency] plastic coated shielded bags used to shield a mobile device from external contact. The bags are coupled with a conductive mesh to provide secure transportation to the laboratory." David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices For Use*

---

[80] *Available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

in Criminal Investigations, Forensic Focus, Aug. 20, 2011.[81] One potential disadvantage of the bag is that the phone can continue to search for a signal, potentially draining the battery while being transported to the laboratory. One possible solution is to hook the phone up to what is called a trickle charger, a small charging device that can be placed within the Faraday bag with the phone. Greg Gogolin, *Digital Forensics Explained* 59-60 (2013). It is also possible that the phone's location data can be overwritten during transport, but the Faraday bag will prevent a remote wiping command from being executed.

One company, Paraben, makes what it calls "Wireless Stronghold Bags 2.0," which it claims is more than 99.999% effective in blocking wireless signals across multiple frequencies. The basic Paraben cellphone bag is available for $39.95. Paraben, *Wireless Stronghold Bags 2.0* (2013).[82]

Aluminum Foil

The main component in a Faraday bag is aluminum foil and so the effect can be replicated simply through wrapping the phone in aluminum foil.

---

[81] *Available at* http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/.

[82] https://www.paraben.com/downloads/sh-bag-brochure.pdf.

The police officer can cover the phone in foil, thus preventing the cell phone from receiving a network signal and executing a remote wiping command. Eamon P. Doherty, *Digital Forensics for Handheld Devices* 14 (2013). The primary disadvantage with the aluminum foil is that its effectiveness has not been tested as fully as Faraday bags; Faraday bags are thus preferred over aluminum foil because the use of foil "could offer an unwanted line of questioning in court." *Id.*

Furthermore, when police have seized the phone and prevented it from receiving a network signal, there is a broad array of tools available to extract data. Modern Data Extraction Devices are capable of obtaining many types of information from personal electronic devices such as cellphones, tablets, and GPS. They can bypass lockscreen and password protections, and recover information that has been previously deleted. A company called Cellbrite makes a device called the Universal Forensics Extraction Device ("UFED") Touch Ultimate that is capable of recovering a wide variety of data files. The device can recover "existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes, etc." Cellbrite, *UFED TOUCH Ultimate: All-inclusive Mobile Forensic Solution* (2013).[83] The device is designed to be compatible with a wide range of phones on the

[83]http://www.cellebrite.com/images/stories/brochures/UFED-Touch-Ultimate-ENGLISH-web.pdf.

market, including Blackberry, IOS, Android phones, and Windows Phones. *Id.*

Pareben Corporation sells a produce called Device Seizure that is preferred by many forensic investigators "because it has some capability to collect information from cell phones, PDAs, and some GPS devices for use in the car. Companies that wish to save money often look for one product that can do more than one purpose…" Eamon P. Doherty, *Digital Forensics for Handheld Devices* 18 (2013).

B. Similar Security Procedures Have Already Been Adopted by Federal Agencies to Protect Sensitive Data in Other Contexts

The federal government has already adopted a number of security protocols to protect sensitive data, similar to the use of signal-blocking packages discussed above. It is clear from existing agency procedures that it would not be unreasonably burdensome to implement similar procedures to protect sensitive cell phone data pending a judicial determination on any warrant application.

In 2004, the State Department announced a plan to install Radio Frequency Identification ("RFID") chips in all newly issued passports. The RFID technology would allow State Department officials to obtain the passport holder's identifying information using radio waves read from a distance but would also allow others to access the content of the passport.

EPIC and other privacy experts and security researchers opposed this proposal, noting that this

technique would unnecessarily expose traveler's sensitive personal information to others, and that technical measures could be adopted to minimize the risk. *See See* Comments of Electronic Privacy Information Center to State Dep't, Dkt. No. DOS-2006-0329 (2007) (RFID tags "creates significant security and privacy risks, particularly if individuals are not able to control the disclosure of identifying information").[84] *See also* Bruce Schneier, Opinion, *Does Big Brother Want to Watch?: Passport Radio Chips Send Too Many Signals*, N.Y. Times, Oct., 4, 2004 ("Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot off this is that travelers carrying around RFID passports are broadcasting their identity").[85]

Privacy groups argued that the use of contactless technology (where the passports could be read through the air rather than being swiped) left the passports vulnerable to surreptitious, unauthorized access from users who possessed compatible readers. Letter from Electronic Frontier Foundation, EPIC, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum to Legal Division Chief, Office of Passport Policy, Planning and Advisory Services, U.S. Dep't of State (April 4, 2005).[86] Furthermore, the RFID technology would

---

[84] *Available at* http://www.epic.org/privacy/us-visit/comm120605.pdf.

[85] *Available at* http://www.nytimes.com/2004/10/04/opinion/04iht-edschneier_ed3_.html.

allow unauthorized users to engage in clandestine tracking of the passport holder via the unique ID numbers attached to each RFID chip. *Id.* at 12. Finally, a lack of encryption left a host of valuable identity information, including biometric data, vulnerable to exfiltration. *Id.* at 13.

In response, the State Department adopted the recommendations of privacy and security experts, and amended the protocol to include an RFID-shielded sleeve in the passport, which prevents remote scanning when the passport is closed. U.S. Dep't of State, *Bureau of Consular Affairs*.[87] The State Department also encrypted the data on the chip and put the key for the encryption on the passport. The new process involved a contact technology whereby "a customs officer swipes the passport through the optical reader to get the key, and then the RFID reader uses the key to communicate with the RFID chip." Bruce Schneier, *Fatal Flaw Weakens RFID Passports*, Wired (Nov. 3, 2005).[88]

These changes to improve the security of the passport information demonstrate the capacity of the government to implement technological measures that protect sensitive personal data from wireless access. A Faraday bag would be a far less expensive technique for securing a seized cell phone than was

---

[87]http://travel.state.gov/content/passports/english/passports/information/card.html.

[88]http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69453?currentPage=all

the State Department's decision to redesign the passport to address concerns about remote access.

The government also has the capacity to protect sensitive information through the use of specially constructed rooms, built to high standards. These are called Sensitive Compartmented Information Facilities ("SCIFs") and are present throughout the government to protect information that has a high security requirement. Many government agencies utilize these facilities, both to store sensitive information and to create a space in which this information can be discussed. Adamo Construction, Inc., *What is a SCIF or Sensitive Compartmented Information Facility?* (2014).[89] SCIFs have substantial construction requirements, which are laid out in Intelligence Community Directive (ICD) 705/IC Technical Specification.[90] SCIFs can either be permanent structures or mobile and temporary depending on the needs of the user. In either case, the materials used in construction of the facility are chosen to prevent electronic signals from either entering or exiting the secured location. In the case of mobile SCIFs, such as the ones utilized by the President while overseas, a shielded tent provides sufficient protection from electronic surveillance.

---

[89] http://www.adamoconstruction.com/what-is-scif.php.

[90] Office of the National Counterintelligence Executive, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.2* (2012), *available at* http://www.fas.org/irp/dni/icd/ics-705-ts.pdf.

Rajini Vidyanathan, *Barack Obama's Top Secret Tent*, BBC News (March 22, 2011).[91]

Such methods demonstrate the ready availability of techniques that would allow the police to preserve evidence on a cell phone so that a warrant may be obtained prior to the search of a device containing, and providing access to, an extraordinary amount of detailed, personal information.

[91] http://www.bbc.co.uk/news/world-us-canada-12810675.

CONCLUSION

For the foregoing reasons, *amicus* respectfully ask this Court to reverse the decision of the California Court of Appeal below.

Respectfully submitted,

MARC ROTENBERG
GINGER MCCALL
ALAN BUTLER
DAVID HUSBAND
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

March 10, 2014