ALAN J. BUTLER, SBN 281291
butler@epic.org
MARC ROTENBERG
AIMEE THOMSON
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009
Telephone: 202.483.1140
Facsimile: 202.483.1248

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	ED No. CM 16-10 (SP) **BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND EIGHT CONSUMER PRIVACY ORGANIZATIONS.** **Hearing:** Date: March 22, 2016 Time: 1:00 p.m. Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym

TABLE OF CONTENTS

Table of Authorities

Cases

Other Authorities

INTEREST OF THE *AMICUS*

This brief is submitted on behalf of several Consumer Privacy Organizations who seek to protect consumers from data breach, financial fraud, and identity theft. The Consumer Privacy Organizations associated with the EPIC *amicus* brief believe that a court order to compel Apple to develop a technique to break security features designed to keep out third parties will result in an increase in crime against consumers.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC was specifically established to advocate for the use of strong encryption technology and for the development of related Privacy Enhancing Technologies. EPIC led the effort in the United States in the 1990s to support strong encryption tools and played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information. EPIC also published the first comparative studies of international encryption policy. *See* EPIC *Cryptography and Liberty 1998: An International Survey of Encryption Policy* (1998).

The Center for Digital Democracy ("CDD") is one of the leading consumer protection and privacy organizations in the United States.[8] Since its founding in 2001, CDD has been at the forefront of research, public education, and advocacy protecting consumers in the digital age.

[8] Center for Digital Democracy, https://www.democraticmedia.org/.

Constitutional Alliance is privately funded nonpartisan non-profit organization whose stated mission is "preserve state and national sovereignty, and the unalienable rights to life, liberty, and the pursuit of happiness as pronounced in the Declaration of Independence and protected under the Bill of Rights of the United States of America."[9]

Consumer Action empowers underrepresented consumers nationwide to assert their rights in the marketplace and financially prosper through multilingual financial education materials, community outreach, and issue-focused advocacy.[10]

Consumer Watchdog is a nonprofit organization dedicated to educating and advocating on behalf of consumers for over 25 years.[11] Its mission is to provide an effective voice for the public interest. Consumer Watchdog's programs include health care reform, oversight of insurance rates, energy policy, protecting privacy rights, protecting legal rights, corporate reform, and political accountability.

The Cyber Privacy Project researches and educates the public about privacy issues raised in today's networked world.[12]

Patient Privacy Rights ("PPR") works to empower individuals and prevent widespread discrimination based on health information using a grassroots, community organizing approach.[13] PPR educates consumers, champions smart policies, and exposes and holds industry and the government accountable.

---

[9] Constitutional Alliance, http://constitutionalalliance.org/.
[10] Consumer Action, http://www.consumer-action.org/.
[11] Consumer Watchdog, http://www.consumerwatchdog.org/.
[12] Cyber Privacy Project, http://cyberprivacyproject.org/.
[13] Patient Privacy Rights, https://patientprivacyrights.org/.

The Privacy Rights Clearinghouse ("PRC") is a nonprofit consumer education and advocacy organization based in San Diego, California.[14] Established in 1992, the PRC focuses on consumers' rights and interests relating to informational privacy, answers individual consumer inquiries, and maintains a robust website of practical privacy protection tips.

Privacy Times provides accurate reporting, objective analysis and thoughtful insight into the events that shape the ongoing debate over privacy and Freedom of Information. [15]

[14] Privacy Rights Clearinghouse, https://www.privacyrights.org/.
[15] Privacy Times, http://www.privacytimes.com/.

INTRODUCTION

The Court's decision in this case will have implications far beyond one investigation, one mobile device, or one company. The security of cell phones is of critical importance to millions of consumers who rely on these devices to protect their most sensitive personal data. As the theft of consumer devices continues to rise—millions of cell phones are stolen every year—the associated crimes of financial fraud and identity theft also increase. Consumers rely on engineers, researchers, and technology companies to develop robust data protection techniques. The security features on mobile devices, such as the Apple iPhone, limit the opportunities for crime that has caused enormous financial, reputational, and emotional harm to consumers across the country. If these safeguards are weakened, consumers will suffer, crime will increase, and the work of law enforcement will be made more difficult.

Technology companies, most notably Apple, have devoted time, energy, and resources to the development of robust security techniques that protect cell phone users from criminal attacks, espionage, stalking, identity theft, harassment, and financial fraud. These efforts should not be in vain. If the Court orders Apple to develop techniques that deactivate the core security features on the iPhone, every iPhone user and every individual whose personal data is stored on an iPhone could be impacted. When it comes to this type of technology, "Either everyone gets security or no one does." Bruce Schneier, *Why You Should Side With Apple, Not the FBI, In the San Bernardino Case*, Wash. Post (Feb. 18, 2016).[16]

[16] https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/.

Modern cell phones are ubiquitous; they are integral to our personal, professional, and educational activities. As Chief Justice John Roberts recently stated for a unanimous Supreme Court, these devices are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484, 189 L. Ed. 2d 430, 441 (2014). The Supreme Court recently found that modern phones store so much sensitive data, which implicates such broad privacy interests, that they deserve special constitutional protections. *Riley*, 134 S. Ct. at 2494.

But protecting these devices from criminals and others who seek to exploit valuable personal data requires more than just legal protection. Data protection requires robust encryption and other security techniques to prevent third parties from gaining access to the contents of a person's cell phone. Consumers demand such protections, and Apple has responded by creating strong digital locks that are designed to keep all others, even Apple, from accessing the contents of a smartphone. Like traditional locks, these devices protect consumers from crime and reduce the risk of theft. And, like traditional locks, they are always subject to attack by determined criminals. This Court should not order Apple or any company to weaken their digital locks because, if they do, consumers will suffer, crime will increase, and any short-term benefit that the Bureau may obtain in this case will be more than outweighed by the increase in crime across the country that will result.

ARGUMENT

The security features in dispute in this case were adopted to protect consumers from crime. Several million phones are stolen every year in the United States. Apple developed specific technical measures to protect the phone so that even Apple could not gain access to its contents. An order to compel Apple to take extraordinary measures to undo these features places at risk millions of cell phone users across the United States.

I. Cell phones are a primary target for criminals and identity thieves.

The theft of cell phones in the United States is now a top concern of policymakers and law enforcement officials. According to the Chairman of the Federal Communications Commission, the agency tasked with regulating the nation's communications services, smartphone theft "is a global problem that causes real harm in a variety of ways. It results in the loss of valuable devices, it often entails physical harm to the victim of the theft, and it can lead to disclosure of vital and confidential personal information stored on the stolen devices." Statement of FCC Chairman Tom Wheeler on Release of Mobile Device Theft Prevention Report by the FCC Technical Advisory Council (Dec. 9, 2015).[17]

Smartphone theft was so widespread by 2012 that the Federal Communications Commission, in consultation with congressional leaders and state law enforcement agencies, developed strategies to curb the problems of "massive smartphone and data theft" and the resulting harms to consumers. FCC, Press Release, *Chairman*

[17] http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1209/DOC-336779A1.pdf.

Genachowski Joins Senator Schumer, D.C. Mayor Gray, State Police Departments, and Wireless Carriers to Announce New Initiatives to Combat Massive Smartphone & Data Theft (Apr. 10, 2012) [hereinafter FCC Initiatives 2012].[18] Nevertheless, smartphone theft nearly doubled from 1.6 million devices in 2012 to 3.1 million devices in 2013. Consumer Reports, *Smart Phone Thefts Rose to 3.1 Million In 2013* (May 28, 2014).[19] Theft was so widespread that it "inspired a new category of crime: 'Apple Picking.'" Office of the N.Y. State Att'y Gen., *Secure Our Smartphones Initiative: One Year Later* i (2014).[20]

Cell phone theft is one of the top priorities for law enforcement officials in most major U.S. cities. Nearly half of all robberies in New York City and more than one third in other major cities involve cell phones. FCC Initiatives 2012, *supra*. Smartphone theft is also an important source of funding for criminal syndicates and terrorist groups. *See* David Gewirtz, *Smartphone Theft Reaches Pandemic Proportions (And You Are A Target)*, ZDNet (Feb. 17, 2014).[21]

The potential cost of stolen and lost phones in the United States was estimated at $30 billion in 2012, and that was prior to rapid rise of phone theft in 2013. Lookout, *Lookout Projects Lost and Stolen Phones Could Cost U.S. Consumers Over $30 Billion in 2012* (Mar. 22, 2012).[22]

---

[18] *Available at* https://www.fcc.gov/document/announcement-new-initiatives-combat-smartphone-and-data-theft.
[19] http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.
[20] http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf.
[21] http://www.zdnet.com/article/smartphone-theft-reaches-pandemic-proportions-and-you-are-a-target/.
[22] https://www.lookout.com/news-mobile-security/lookout-lost-phones-30-billion.

The risk of smartphone theft affects the vast majority of consumers in the United States. Roughly 72% of American adults own a smartphone, compared to more than 40% of adults worldwide, and that number rises to 92% for the 18-34 demographic. Jacob Poushter, *Smartphone Ownership and Internet Useage Continues to Climb in Emerging Economies*, PewResearchCenter (Feb. 22, 2016).[23] It is estimated that one in ten smartphone owners are victims of theft. Lookout, *Phone Theft in America* (2016).[24]

Victims of phone theft not only bear the cost of replacing their devices, they also lose valuable personal data and face an increased risk of identity theft. At least half of phone theft victims would pay at least $500 just to recover their stolen data, and one-third would pay as much as $1,000. *Id*. But the loss of irreplaceable files and the price of a new device are not the only costs of phone theft. An estimated 10% of phone theft victims subsequently suffer identity theft. *Id.* Victims of identity theft lost an average of $1,500 per person in 2012, but the true cost of identity theft "is complex and involves more than the dollars lost" because it can impact your credit and require countless hours spent identifying and resolving fraudulent transactions. Kimberly Rotter, *The Staggering Costs of Identity Theft in the U.S.*, Credit Sesame (June 19, 2014).[25] Some consumers are so desperate to recover their lost phones that they have attempted to track down and confront the criminals themselves, which can be

[23] http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.
[24] https://www.lookout.com/resources/reports/phone-theft-in-america.
[25] http://www.creditsesame.com/blog/staggering-costs-of-identity-theft/.

dangerous and lead to additional risks. *See* Ian Lovett, *When Hitting 'Find My iPhone' Takes You to a Thief's Doorstep*, N.Y. Times (May 3, 2014).[26]

Given the opportunity, thieves who obtain a victim's phones will gain access to the person's sensitive data. A study by a leading security firm confirmed that a majority of individuals who obtain an unprotected phone will attempt to access sensitive files and applications. Symantec, *The Symantec Smartphone Honey Stick Project* 11 (2012).[27] The study found that after intentionally losing smartphones with special tracking software installed, there were attempts to access the personal, corporate, and other data on those phones in the vast majority of cases. This included data stored in "personal" materials such as social networking apps, online banking apps, webmail, and photos (accessed in 89% of cases) as well as "corporate" materials such as remote administration apps, human resources records, and corporate e-mail apps (accessed in 83% of cases). *Id*.

State and federal law enforcement agencies have committed significant resources to promoting security features on cell phones that protect victims and consumers. *See* Office of the N.Y. State Att'y Gen., *Secure Our Smartphones Initiative: One Year Later* i (2014). As early as 2013, law enforcement groups were urging device manufacturers to develop and improve technologies that deter crime. As the director of the Police Executive Research Forum noted at the time, "If you look at auto theft, it has really plummeted in this country because technology has advanced so

[26] http://www.nytimes.com/2014/05/04/us/when-hitting-find-my-iphone-takes-you-to-a-thiefs-doorstep.html?_r=3.

[27] https://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf.

much and the manufacturers recognize the importance of it." Brian X. Chen & Malia Wollan, *Cellphone Thefts Grow, but the Industry Looks the Other Way*, N.Y. Times (May 1, 2013).[28] Law enforcement groups lamented that "The cellphone industry has for the most part been in denial. For whatever reasons, it has been slow to move." *Id*. In response to the requests of law enforcement agencies, device manufacturers have since developed security features that protect sensitive data and deter theft. These new security features are precisely the type of software controls that would be put at risk by the Court's order.

II. Device manufacturers developed smartphone security features in conjunction with law enforcement to protect consumers from theft.

Following the steep increase in smartphone theft, as well as the urgings of lawmakers and law enforcement officials, Apple and other device manufacturers developed several new features to protect consumers. First, the companies have introduced stronger passcodes that make it harder for a criminal to gain unauthorized access to the phone. Cadie Thompson, *Apple Made A Simple Change in iOS 9 That Will Make Your iPhone A Lot Safer*, TechCrunch (Sept. 16, 2015).[29] Second, companies have restricted certain external functions (such as data sync) to "trusted" devices only. *See* Apple, *About The 'Trust This Computer' Alert on Your iPhone, iPad, or iPod Touch* (2016).[30] And third, the companies have created activation blocking features that

[28] http://www.nytimes.com/2013/05/02/technology/cellphone-thefts-grow-but-the-industry-looks-the-other-way.html.
[29] http://www.techinsider.io/ios-9-defaults-to-6-digit-passcode-2015-9.
[30] https://support.apple.com/en-us/HT202778.

prevent stolen phones from being reused after an illicit sale. Consumer Reports, *Smartphone Thefts Drop As Kill Switch Usage Grows* (June 11, 2015).[31]

These security features are not only beneficial to consumers, they reduce the risk of crime and are now legally required in some states such as Minnesota and California. *Id*. Law enforcement agencies actively campaigned for these stronger security measure, ultimately building a "broad-based, international coalition of more than 100 elected leaders, attorneys general, consumer advocates, and top law enforcement officials from major cities." Office of the N.Y. State Att'y Gen., *Secure Our Smartphones Initiative: One Year Later* (2014). The FCC also established the Mobile Device Theft Prevention working group in 2012 to put device manufacturers in contact with "law enforcement and government representatives for the interests of the consumer." Statement of FCC Chairman Tom Wheeler on Release of Mobile Device Theft Prevention Report by the FCC Technical Advisory Council (Dec. 9, 2015). And for good reason. One study estimated that anti-theft software could save consumers $3.4 billion per year. Consumer Reports, *Smartphone Thefts Drop As Kill Switch Usage Grows* (June 11, 2015).

The Federal Communications Commission reported in 2014 that there had already been a sharp decline in Apple iPhone thefts as a result of the use of new security features. *See* FCC, *Report of Technical Advisory Council (TAC) Subcommittee*

[31] Apple has adopted other Privacy Enhancing Techniques, such as methods for anonymizing user identity to reduce risk of spoofing and identity theft, and end-to-end encryption for iMessage to reduce the risk of communications interception.

on Mobile Device Theft Prevention (MDTP) 25 (Dec. 4, 2014).[32] All the three major cities tracked by the FCC, in coordination with the states' attorneys general, showed significant reductions in iPhone theft following the release of the new security features. In New York City, where smartphone thefts had been steadily on the rise for three years, rates of both "robberies and grand larcenies from a person involving Apple products" dropped the year after the new security features were enabled by "19 percent and 29 percent, compared to the same time period in the previous year." *Id*. Similar results were seen in San Francisco where "Apple smartphones constituted the vast majority" of phones stolen and robberies "declined 38%" in the six months after the features were enabled. *Id*. Reports from London also confirmed that these techniques were effective at deterring crime, with a 24% reduction in iPhone theft in the six months after the features were enabled. *Id*.

The Court should not adopt an order that could undo much of the work that device manufacturers, consumer advocates, federal and state law enforcement agencies, and legislatures have achieved to establish data protection for cell phones.

III. The court order will undermine the security and personal safety of cell phone users.

An order to Apple to undo the security features that protect consumers will increase the risk of cell phone theft and literally open doors for new criminal opportunities, such as the remote deactivation of door locks that safeguard consumers in their homes.

[32] http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf.

A. Smartphones store a wealth of sensitive files and communications.

Cell phones are no longer simple communications devices used to send and receive calls. The majority of phones are 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. Consumers now use many different mobile apps on their cell phones to access personal data. In 2014, over 91% of smartphone users installed at least one app on their phone. *Only 33% of US Mobile Users Will Pay for Apps This Year*, eMarketer (Feb. 5, 2015).[33] The average smartphone user accessed 26.7 apps per month by the end of 2014. *So Many Apps, So Much More Time for Entertainment*, Nielson (June 11, 2015).[34] Approximately 89% of mobile media time is spent on apps. Stacey Rudolph, *Mobile Apps Usage – Statistics and Trends [Infographic]*, (June 15, 2015).[35] There are now more than 1.5 million different apps available for Apple devices. Statista, *Number of Available Apps in the Apple App Store from July 2008 to June 2015* (2016).[36] These programs enable users to access a variety of services and download up-to-date information.

[33] http://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965#sthash.2iaYCGit.dpuf.
[34] http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html.
[35] http://www.business2community.com/infographics/mobile-apps-usage-statistics-trends-infographic-01248837#K6VUYPJKG1UcyiT8.99.
[36] http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/.

Medical Records

Many users rely on their cell phones to access sensitive medical information. Some of these applications provide complete access to medical history files that include private 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. Medicare, *Download Claims with Medicare's Blue Button*.[37] Third party applications also help patients and doctors manage records and treatments online. For example, Drchrono is an "integrated practice management, electronic health record & medical billing platform" built for the iPad, iPhone, and Apple Watch. *drchrono* (2016).[38] Drchrono integrates with the remote file server Box, allowing patients and doctors to share files via third party servers. drchrono, *Box* (2016).[39] Other applications allow users to log information about their fitness habits, nutritional intake, menstrual cycles, blood pressure, and medication times. According to Pew Research, 19% of smartphone users have a health app on their phone. Susannah Fox & Maeve Duggan, *Mobile Health 2012*, PewResearch Internet Project.[40]

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 their personal information might be at risk when using a mobile device to access health records or tests online. Deloitte Consulting, *mHealth: a*

---

[37] https://www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html (last visited Mar. 2, 2016).
[38] https://www.drchrono.com/.
[39] https://www.drchrono.com/partners/box/.
[40] http://www.pewinternet.org/fact-sheets/health-fact-sheet/ (last visited Mar. 2, 2016).

Check-up on Consumer Use (2014).[41] Apple and other device manufacturers have responded to these concerns, creating new features to secure sensitive health data. Apple. *Approach to Privacy* (2016).[42]

Messaging Services

Mobile phone users rely on a variety of applications to send electronic communications. Gmail has more than one billion active email users, 75% of whom access their email accounts on mobile devices. Frederic Lardinois, *Gmail Now Has More Than 1B Monthly Active Users*, TechCrunch (Feb 1., 2016).[43] Gmail account holders can use the Gmail app to access their emails stored in the cloud. Google, *Overview of the Gmail App (iPhone & iPad)* (2016).[44] The user (or anyone controlling the phone) accesses messages by either scrolling down or conducting a keyword search in the app. *Id*.

Mobile phones also provide access to online social networking accounts. Most social networking services also offer private messaging services. Facebook, the most popular service with 1.04 billion daily active users, Facebook, *Stats* (2016),[45] allows users to communicate privately via an instant messaging tool and an email-like messaging function, Facebook, *Managing Messages* (2016).[46] Twitter, which has 320 million monthly active users, 80% of which use their phone to tweet, Twitter,

---

[41] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-chs-mhealth-infographic.pdf.
[42] http://www.apple.com/privacy/approach-to-privacy/.
[43] http://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/.
[44] https://support.google.com/mail/answer/1205704?hl=en.
[45] http://newsroom.fb.com/company-info/.
[46] https://www.facebook.com/help/www/336759363070078/.

Company Facts (2016),[47] allows users to publicly post text or picture messages ("tweets") or to send private, "direct messages" to other users, Twitter, *Getting Started With Twitter* (2016).[48]

Photos and Videos

One of the key features of the iPhone and other mobile devices is the built-in photo and video camera. *See* Apple, *iPhone 6s Cameras* (2016).[49] These devices enable users to create and store files that can include images of family members or other private matters. Apple also has a built-in photo-sharing feature for iPhone users. *See* Apple, *iCloud Photo Sharing* (2016).[50] This app allows users to create and share photos with other users, and "[a]ny edits you make are automatically updated everywhere." *Id*. Users even get "real-time notifications" when someone joins an album, posts a photo, or makes a comment. *Id*. This means that at any time a users phone could automatically receive new private photos from their friends, without even opening the app. Anyone who has access to a user's phone could also browse or download these private photos.

Library Records

Individuals increasingly use their smartphones to access books, films, music, and databases available from their library, and to keep records of their library use. Third-party library apps—such as Overdrive , Hoopla, Freegal, OneClickDigital, and 3M —allow library users to borrow or stream content and store a record of the books,

[47] https://about.twitter.com/company.
[48] https://support.twitter.com/articles/215585.
[49] http://www.apple.com/iphone-6s/cameras/.
[50] https://www.apple.com/icloud/photos/.

music, and movies accessed through these apps. Over 90 libraries and library systems have taken the next step and provide dedicated apps for the iPhone that integrate the library's circulation system with its public catalogs and the user's library records.

Remote File Storage

Remote file storage services allow users to store, access, edit, and share their files, including word processing documents, presentations, spreadsheets, pictures, music, and videos. Many of these file storage services can be accessed remotely from mobile apps installed on a smartphone. These files are private and can include a great deal of sensitive personal information—financial records, private messages, photographs, personal notes, and health records.

Financial Records & Transactions

Consumers are increasingly pursuing services "that allow consumers to obtain financial account information and conduct transactions with their financial institution ('mobile banking') and that allow consumers to make payments, transfer money, or pay for goods and services ('mobile payments')." Bd. of Gov's of the Fed. Reserve Sys., *Consumer and Mobile Financial Services 2015*, at 5 (Mar. 2015).[51] In 2014, 39% of mobile phone users and 52% of smartphone users with bank accounts used mobile banking apps while 22% of mobile phone users and 28% of smartphone users used mobile payment apps. *Id.* Many banks have dedicated apps that provide their

[51] https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf

customers with mobile account access. *See*, *e.g.*, Bank of America, *Mobile Banking* (2016);[52] Wells Fargo, *Apps* (2016);[53] Chase, *Mobile Banking* (2016).[54]

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. Mint, *How it Works* (2016).[55] And transactional apps, such as Uber, PayPal, and Venmo, typically store bank or credit card information, allowing for automatic payments.

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, e.g.*, Citrix, *GoToMyPC* (2016).[56] 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* (2012).[57] These apps are especially popular with employers because they can be used to "[i]ncrease employee productivity and flexibility." *Id*.

---

[52] https://www.bankofamerica.com/online-banking/mobile.go.
[53] https://www.wellsfargo.com/mobile/apps/.
[54] https://www.chase.com/online/digital/mobile-banking.html.
[55] https://www.mint.com/how-mint-works.
[56] https://www.citrix.com/products/gotomypc/overview.html.
[57] http://www.gotomypc.com/remote_access/images/pdf/GoToMyPC_Mobile_App_Factsheet.pdf.

B. Smartphones also serve as an authenticator and key to many sensitive accounts and services

Smartphones not only store and provide access to a wealth of sensitive data, they also act as a key to access a user's many accounts—social media accounts, bank accounts, e-mail accounts, and other profiles. Users are typically required to create unique, complex passwords for these accounts. But most people struggle to create and remember strong passwords. *See* Troy Hunt, *The Only Secure Password is the One You Can't Remember*, Lifehacker (Mar. 24, 2011);[58] 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.").[59]

Smartphones provide an attractive solution to this problem: storing passwords and other login information on the device so that the user can access protected services without repeatedly entering the complex password. For example, Apple has built a password storage system into the iPhone. *See* Apple, *Frequently Asked Questions About iCloud Keychain* (2015) ("iCloud Keychain keeps your Safari website usernames and passwords, credit card information, and Wi-Fi network information up to date across all of your approved devices."). Some mobile apps also keep users logged in by default. Other apps provide storage of user login information for many

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

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

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+ (Apr. 15, 2013).[60] For example, when a user logs into Facebook on their iPhone, 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* (2016);[61] Facebook, *How Do I Log Out of The Iphone or Ipad App?* (2016).[62] Many users rely on these features, but the convenience of automatically logging in to an app or account also makes it easier for a criminal or third party to gain unauthorized access.

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). The user enters the passwords for all the websites and applications they wish to use, including banking, medical, and other extremely sensitive accounts. These passwords are secured by a

---

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

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

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

master password. As with the in app storage of passwords, the password manager provides access to sensitive accounts and data not stored on the phone.

In addition to storing passwords that provide access to a user's online accounts, smartphones also provide a mechanism to verify a user's identity. This type of authentication, commonly referred to as "two-factor authentication," is becoming standard for many online accounts. *See* Michelle Maisto, *Google Nudges Customers Toward Two-Factor Authentication*, InformationWeek (Mar. 2, 2016).[63] The process works by sending the user a unique code in a text message, or requiring the user to input a code generated by an authenticating app (e.g. RSA SecureID Software Token for iOS or Google Authenticator). This adds an extra layer of security for online accounts, but also makes the smartphone a key target for criminals, identity thieves, and intelligence agencies. *See The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 11 (2016) (testimony of Susan Landau, Professor, Worcester Polytechnic Institute)[64] (noting that "the most valuable data for attackers is your login credentials").

C. Smart phones enable access to a person's home and control over the appliances within the home

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

[63] http://www.informationweek.com/software/productivity-collaboration-apps/google-nudges-customers-toward-two-factor-authentication/d/d-id/1324502.
[64] http://judiciary.house.gov/_cache/files/b3af6e9e-b599-4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf.

other utilities. Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything* 9 (2014).[65]

For example, General Electric offers a range of wi-fi-connected ovens, refrigerators, dishwashers, and laundry machines that users can control with mobile apps. General Electric, *GE Wifi Connect* (2016).[66] Nest, recently acquired by Google, has devised the Nest Thermostat, which "learns what temperature you like and builds a schedule around yours." Nest, *Meet the Nest Thermostat* (2016).[67] Other Nest products include a smoke alarm that can send mobile alerts to your phone, Nest, *Meet Nest Protect* (2016),[68] and a security camera with 24/7 live streaming and activity alerts, Nest, *Meet Nest Cam* (2016).[69] The Nest App allows a user to "change the temperature or view your energy usage on your Nest Thermostat, get smoke and carbon monoxide alerts from your Nest Protect, watch Nest Cam video footage, and much more." Nest, *Learn More About What You Can Do With The Nest App* (July 14, 2015).[70]

Companies have even begun offering digital door locks that can be unlocked using an iPhone or other mobile device. *See* August, *August Smart Lock* (2015);[71] Kwikset, *Kevo Smart Lock* (2016).[72] Smartphones can similarly be used to deactivate a

---

[65] https://www.wi-fi.org/system/files/wp_Wi-Fi_Internet_of_Things_Vision_20140110.pdf.
[66] http://www.geappliances.com/ge/connected-appliances/.
[67] https://nest.com/thermostat/meet-nest-thermostat/?alt=3.
[68] https://nest.com/smoke-co-alarm/meet-nest-protect/.
[69] https://nest.com/camera/meet-nest-cam/.
[70] https://nest.com/support/article/Learn-more-about-the-Nest-app.
[71] http://august.com/products/august-smart-lock/.
[72] http://www.kwikset.com/kevo/default.aspx#.Vti3YZMrL-Y.

user's home security system, open their garage door, and control other home security features. Livewatch, *Controlling Your Alarm System from Your Smart Phone* (2016).[73]

* * *

The security features in smartphones are essential to protecting sensitive personal information, and services that can be unlocked using the devices. Encryption is the cornerstone of computer security. As EPIC warned almost twenty years ago:

> Governmental regulation of cryptographic security techniques endangers personal privacy. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail. In a networked environment, such information is increasingly at risk of being stolen or misused.

EPIC, *Cryptography & Liberty 1999: An International Survey of Encryption Policy* (1999). But it was the framers of the Constitution who first made clear that security is a fundamental right of individuals. U.S. Const. amend. IV ("The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." (emphasis added)).

[73] https://www.livewatch.com/control-alarm-system-with-smartphone.

CONCLUSION

For the foregoing reasons, the *amicus* respectfully requests that this Court grant Apple's motion to vacate the order compelling assistance.

Dated: March 3, 2016

Respectfully submitted,

By: /s/ *Alan J. Butler*
ALAN J. BUTLER

Marc Rotenberg
Aimee Thomson
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)
Attorneys for Amicus Curiae