

1 ALAN J. BUTLER, SBN 281291
butler@epic.org
2 MARC ROTENBERG
3 AIMEE THOMSON
ELECTRONIC PRIVACY INFORMATION CENTER
4 1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009
5 Telephone: 202.483.1140

6 Facsimile: 202.483.1248 UNITED STATES DISTRICT COURT

7
8 CENTRAL DISTRICT OF CALIFORNIA

9 EASTERN DIVISION

10 IN THE MATTER OF THE
11 SEARCH OF AN APPLE IPHONE
SEIZED DURING THE
12 EXECUTION OF A SEARCH
WARRANT ON A BLACK LEXUS
13 IS300, CALIFORNIA LICENSE
PLATE 35KGD203
14

ED No. CM 16-10 (SP)
BRIEF OF *AMICUS CURIAE*
ELECTRONIC PRIVACY
INFORMATION CENTER
(EPIC) AND EIGHT
CONSUMER PRIVACY
ORGANIZATIONS.

15 **Hearing:**

16 Date: March 22, 2016
17 Time: 1:00 p.m.
Place: Courtroom 3 or 4
18 Judge: Hon. Sheri Pym

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICUS* 1

INTRODUCTION 4

ARGUMENT 6

 I. Cell phones are a primary target for criminals and identity thieves. 6

 II. Device manufacturers developed cell phone security features in conjunction
 with law enforcement to protect consumers from theft..... 10

 III. The court order will undermine the security and personal safety of cell
 phone users. 12

 A. Smartphones store a wealth of sensitive files and communications..... 13

 B. Smartphones also serve as an authenticator and key to many sensitive
 accounts and services 19

 C. Smart phones enable access to a person’s home and control over the
 appliances within the home 21

CONCLUSION 24

1
2
3 **Table of Authorities**

4 **Cases**

5 *Riley v. California*, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014)5

6 **Other Authorities**

7 Apple, *Frequently Asked Questions About iCloud Keychain* (2015)19

8 Apple, *iCloud Photo Sharing* (2016).....16

9 Apple, *iPhone 6s Cameras* (2016)16

10 Apple, *Approach to Privacy* (2016)15

11 August, *August Smart Lock* (2015).....22

12 Bank of America, *Mobile Banking* (2016)18

13 Bd. of Gov’s of the Fed. Reserve Sys., *Consumer and Mobile Financial Services 2015*
14 (Mar. 2015)17

15 Brian X. Chen & Malia Wollan, *Cellphone Thefts Grow, but the Industry Looks the*
16 *Other Way*, N.Y. Times (May 1, 2013).....10

17 Bruce Schneier, *Why You Should Side With Apple, Not the FBI, In the San Bernardino*
18 *Case*, Wash. Post (Feb. 18, 2016).....4

19 Cadie Thompson, *Apple Made A Simple Change in iOS 9 That Will Make Your iPhone*
20 *A Lot Safer*, TechCrunch (Sept. 16, 2015)10

21 Chase, *Mobile Banking* (2016)18

22 Citrix, *GoToMyPC* (2016)18

23 Citrix, *GoToMyPC: Total Mobility – Factsheet* (2012)18

24 Consumer Reports, *Smart Phone Thefts Rose to 3.1 Million In 2013* (May 28, 2014)...7

1 Consumer Reports, *Smartphone Thefts Drop As Kill Switch Usage Grows* (June 11,
2 2015) 11
3
4 David Gewirtz, *Smartphone Theft Reaches Pandemic Proportions (And You Are A
5 Target)*, ZDNet (Feb. 17, 2014)..... 7
6
7 Deloitte Consulting, *mHealth: a Check-up on Consumer Use* (2014) 15
8
9 drchrono, *Box* (2016) 14
10 drchrono, <https://www.drchrono.com> (2016) 14
11
12 EPIC, *Cryptography & Liberty 1999: An International Survey of Encryption Policy*
13 (1999) 23
14
15 Facebook, *How Do I Log Out of The Iphone or Ipad App?* (2016) 20
16
17 Facebook, *Managing Messages* (2016) 15
18
19 Facebook, *Stats* (2016) 15
20
21 FCC, Press Release, *Chairman Genachowski Joins Senator Schumer, D.C. Mayor
22 Gray, State Police Departments, and Wireless Carriers to Announce New Initiatives
23 to Combat Massive Smartphone & Data Theft* (Apr. 10, 2012)..... 7
24
25 FCC, Report of Technical Advisory Council (TAC) Subcommittee on Mobile Device
26 Theft Prevention (MDTP) (Dec. 4, 2014) 12
27
28 Frederic Lardinois, *Gmail Now Has More Than 1B Monthly Active Users*, TechCrunch
(Feb 1., 2016) 15
General Electric, *GE Wifi Connect* (2016) 22
Google, *Overview of the Gmail App (iPhone & iPad)* (2016) 15
Ian Lovett, *When Hitting ‘Find My iPhone’ Takes You to a Thief’s Doorstep*, N.Y.
Times (May 3, 2014) 9

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Jacob Poushter, *Smartphone Ownership and Internet Useage Continues to Climb in Emerging Economies*, PewResearchCenter (Feb. 22, 2016).....8

Jonathan Garro, *Mac Computer Skills: Unlock the Power of Your Mac’s Keychain Utility*, Tuts+ (Apr. 15, 2013)20

Kimberly Rotter, *The Staggering Costs of Identity Theft in the U.S.*, Credit Sesame (June 19, 2014).....8

Kit Eaton, *Apps to Protect Your Array of Passwords*, N.Y. Times (Oct. 17, 2013)20

Kwikset, *Kevo Smart Lock* (2016).....22

Livewatch, *Controlling Your Alarm System from Your Smart Phone* (2016)23

Lookout, *Lookout Projects Lost and Stolen Phones Could Cost U.S. Consumers Over \$30 Billion in 2012* (Mar. 22, 2012).....7

Lookout, *Phone Theft in America* (2016)8

Michelle Maisto, *Google Nudges Customers Toward Two-Factor Authentication*, InformationWeek (Mar. 2, 2016)21

Mint, *How it Works* (2016).....18

Nest, *Learn More About What You Can Do With The Nest App* (July 14, 2015)22

Nest, *Meet Nest Cam* (2016).....22

Nest, *Meet Nest Protect* (2016)22

Nest, *Meet the Nest Thermostat* (2016)22

Office of the N.Y. State Att’y Gen., *Secure Our Smartphones Initiative: One Year Later* i (2014).....7, 9, 11

Only 33% of US Mobile Users Will Pay for Apps This Year, eMarketer (Feb. 5, 2015)13

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Phillip Inglesant & M. Angela Sasse, *The True Cost of Unusable Password Polices: Password Use in the Wild*, Proc. SIGCHI Conf. Hum. Factors Comp. Sys. (2010)..19

So Many Apps, So Much More Time for Entertainment, Nielson (June 11, 2015)13

Stacey Rudolph, *Mobile Apps Usage – Statistics and Trends [Infographic]*, (June 15, 2015)13

Statement of FCC Chairman Tom Wheeler on Release of Mobile Device Theft Prevention Report by the FCC Technical Advisory Council (Dec. 9, 2015)6, 11

Statista, *Number of Available Apps in the Apple App Store from July 2008 to June 2015* (2016)13

Susannah Fox & Maeve Duggan, *Mobile Health 2012*, PewResearch Internet Project (Nov. 8, 2012)14

Symantec, *The Symantec Smartphone Honey Stick Project* (2012)9

The Encryption Tightrope: Balancing Americans’ Security and Privacy: Hearing Before the H. Comm. on the Judiciary, 114th Cong. (2016) (testimony of Susan Landau, Professor, Worcester Polytechnic Institute).....21

Troy Hunt, *The Only Secure Password is the One You Can’t Remember*, Lifehacker (Mar. 24, 2011)19

Twitter, *Company Facts* (2016).....16

Twitter, *Getting Started With Twitter* (2016)16

Twitter, *How to Sign Out of Twitter for iPhone* (2016)20

Wells Fargo, *Apps* (2016).....18

Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything* (2014)22

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

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/>.

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

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

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

16 The Cyber Privacy Project researches and educates the public about privacy
17 issues raised in today’s networked world.¹²

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

25 ⁹ Constitutional Alliance, <http://constitutionalalliance.org/>.

26 ¹⁰ Consumer Action, <http://www.consumer-action.org/>.

27 ¹¹ Consumer Watchdog, <http://www.consumerwatchdog.org/>.

28 ¹² Cyber Privacy Project, <http://cyberprivacyproject.org/>.

¹³ Patient Privacy Rights, <https://patientprivacyrights.org/>.

1 The Privacy Rights Clearinghouse (“PRC”) is a nonprofit consumer education
2 and advocacy organization based in San Diego, California.¹⁴ Established in 1992, the
3 PRC focuses on consumers’ rights and interests relating to informational privacy,
4 answers individual consumer inquiries, and maintains a robust website of practical
5 privacy protection tips.
6

7 Privacy Times provides accurate reporting, objective analysis and thoughtful
8 insight into the events that shape the ongoing debate over privacy and Freedom of
9 Information.¹⁵
10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

¹⁴ Privacy Rights Clearinghouse, <https://www.privacyrights.org/>.

28 ¹⁵ Privacy Times, <http://www.privacytimes.com/>.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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/>.

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

9
10
11 But protecting these devices from criminals and others who seek to exploit
12 valuable personal data requires more than just legal protection. Data protection
13 requires robust encryption and other security techniques to prevent third parties from
14 gaining access to the contents of a person’s cell phone. Consumers demand such
15 protections, and Apple has responded by creating strong digital locks that are designed
16 to keep all others, even Apple, from accessing the contents of a smartphone. Like
17 traditional locks, these devices protect consumers from crime and reduce the risk of
18 theft. And, like traditional locks, they are always subject to attack by determined
19 criminals. This Court should not order Apple or any company to weaken their digital
20 locks because, if they do, consumers will suffer, crime will increase, and any short-
21 term benefit that the Bureau may obtain in this case will be more than outweighed by
22 the increase in crime across the country that will result.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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 million 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.

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

11 Cell phone theft is one of the top priorities for law enforcement officials in most
12 major U.S. cities. Nearly half of all robberies in New York City and more than one
13 third in other major cities involve cell phones. FCC Initiatives 2012, *supra*.

15 Smartphone theft is also an important source of funding for criminal syndicates and
16 terrorist groups. See David Gewirtz, *Smartphone Theft Reaches Pandemic Proportions*
17 *(And You Are A Target)*, ZDNet (Feb. 17, 2014).²¹

18 The potential cost of stolen and lost phones in the United States was estimated at
19 \$30 billion in 2012, and that was prior to rapid rise of phone theft in 2013. Lookout,
20 *Lookout Projects Lost and Stolen Phones Could Cost U.S. Consumers Over \$30 Billion*
21 *in 2012* (Mar. 22, 2012).²²

23
24 ¹⁸ Available at <https://www.fcc.gov/document/announcement-new-initiatives-combat-smartphone-and-data-theft>.

25 ¹⁹ <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>.

26 ²⁰ <http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf>.

27 ²¹ <http://www.zdnet.com/article/smartphone-theft-reaches-pandemic-proportions-and-you-are-a-target/>.

28 ²² <https://www.lookout.com/news-mobile-security/lookout-lost-phones-30-billion>.

1 The risk of smartphone theft affects the vast majority of consumers in the United
2 States. Roughly 72% of American adults own a smartphone, compared to more than
3 40% of adults worldwide, and that number rises to 92% for the 18-34 demographic.
4 Jacob Poushter, *Smartphone Ownership and Internet Useage Continues to Climb in*
5 *Emerging Economies*, PewResearchCenter (Feb. 22, 2016).²³ It is estimated that one in
6 ten smartphone owners are victims of theft. Lookout, *Phone Theft in America* (2016).²⁴
7
8

9 Victims of phone theft not only bear the cost of replacing their devices, they also
10 lose valuable personal data and face an increased risk of identity theft. At least half of
11 phone theft victims would pay at least \$500 just to recover their stolen data, and one-
12 third would pay as much as \$1,000. *Id.* But the loss of irreplaceable files and the price
13 of a new device are not the only costs of phone theft. An estimated 10% of phone theft
14 victims subsequently suffer identity theft. *Id.* Victims of identity theft lost an average
15 of \$1,500 per person in 2012, but the true cost of identity theft “is complex and
16 involves more than the dollars lost” because it can impact your credit and require
17 countless hours spent identifying and resolving fraudulent transactions. Kimberly
18 Rotter, *The Staggering Costs of Identity Theft in the U.S.*, Credit Sesame (June 19,
19 2014).²⁵ Some consumers are so desperate to recover their lost phones that they have
20 attempted to track down and confront the criminals themselves, which can be
21
22
23
24
25

26 ²³ <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.

27 ²⁴ <https://www.lookout.com/resources/reports/phone-theft-in-america>.

28 ²⁵ <http://www.creditsesame.com/blog/staggering-costs-of-identity-theft/>.

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

4 Given the opportunity, thieves who obtain a victim’s phones will gain access to
5 the person’s sensitive data. A study by a leading security firm confirmed that a majority
6 of individuals who obtain an unprotected phone will attempt to access sensitive files
7 and applications. Symantec, *The Symantec Smartphone Honey Stick Project 11*
8 (2012).²⁷ The study found that after intentionally losing smartphones with special
9 tracking software installed, there were attempts to access the personal, corporate, and
10 other data on those phones in the vast majority of cases. This included data stored in
11 “personal” materials such as social networking apps, online banking apps, webmail,
12 and photos (accessed in 89% of cases) as well as “corporate” materials such as remote
13 administration apps, human resources records, and corporate e-mail apps (accessed in
14 83% of cases). *Id.*
15
16

17 State and federal law enforcement agencies have committed significant
18 resources to promoting security features on cell phones that protect victims and
19 consumers. See Office of the N.Y. State Att’y Gen., *Secure Our Smartphones*
20 *Initiative: One Year Later i* (2014). As early as 2013, law enforcement groups were
21 urging device manufacturers to develop and improve technologies that deter crime. As
22 the director of the Police Executive Research Forum noted at the time, “If you look at
23 auto theft, it has really plummeted in this country because technology has advanced so
24
25

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

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

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

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

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

26 ²⁸ [http://www.nytimes.com/2013/05/02/technology/cellphone-thefts-grow-but-the-](http://www.nytimes.com/2013/05/02/technology/cellphone-thefts-grow-but-the-industry-looks-the-other-way.html)
27 [industry-looks-the-other-way.html](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>.

1 prevent stolen phones from being reused after an illicit sale. Consumer Reports,
2 *Smartphone Thefts Drop As Kill Switch Usage Grows* (June 11, 2015).³¹
3

4 These security features are not only beneficial to consumers, they reduce the risk
5 of crime and are now legally required in some states such as Minnesota and California.
6 *Id.* Law enforcement agencies actively campaigned for these stronger security
7 measure, ultimately building a “broad-based, international coalition of more than 100
8 elected leaders, attorneys general, consumer advocates, and top law enforcement
9 officials from major cities.” Office of the N.Y. State Att’y Gen., *Secure Our*
10 *Smartphones Initiative: One Year Later* (2014). The FCC also established the Mobile
11 Device Theft Prevention working group in 2012 to put device manufacturers in contact
12 with “law enforcement and government representatives for the interests of the
13 consumer.” Statement of FCC Chairman Tom Wheeler on Release of Mobile Device
14 Theft Prevention Report by the FCC Technical Advisory Council (Dec. 9, 2015). And
15 for good reason. One study estimated that anti-theft software could save consumers
16 \$3.4 billion per year. Consumer Reports, *Smartphone Thefts Drop As Kill Switch*
17 *Usage Grows* (June 11, 2015).
18
19
20

21 The Federal Communications Commission reported in 2014 that there had
22 already been a sharp decline in Apple iPhone thefts as a result of the use of new
23 security features. *See* FCC, *Report of Technical Advisory Council (TAC) Subcommittee*
24
25
26

27 ³¹ Apple has adopted other Privacy Enhancing Techniques, such as methods for
28 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.

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

13
14
15
16 The Court should not adopt an order that could undo much of the work that
17 device manufacturers, consumer advocates, federal and state law enforcement
18 agencies, and legislatures have achieved to establish data protection for cell phones.

19
20 **III. The court order will undermine the security and personal safety of cell**
21 **phone users.**

22 An order to Apple to undo the security features that protect consumers will
23 increase the risk of cell phone theft and literally open doors for new criminal
24 opportunities, such as the remote deactivation of door locks that safeguard consumers
25 in their homes.
26

27
28 ³² <http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf>.

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

2 Cell phones are no longer simple communications devices used to send and
3 receive calls. The majority of phones are sophisticated portable computers that provide
4 constant Internet connectivity and a single point of access to all of the user’s personal
5 files, communications, and records. Consumers now use many different mobile apps
6 on their cell phones to access personal data. In 2014, over 91% of smartphone users
7 installed at least one app on their phone. *Only 33% of US Mobile Users Will Pay for*
8 *Apps This Year*, eMarketer (Feb. 5, 2015).³³ The average smartphone user accessed
9 26.7 apps per month by the end of 2014. *So Many Apps, So Much More Time for*
10 *Entertainment*, Nielsen (June 11, 2015).³⁴ Approximately 89% of mobile media time is
11 spent on apps. Stacey Rudolph, *Mobile Apps Usage – Statistics and Trends*
12 *[Infographic]*, (June 15, 2015).³⁵ There are now more than 1.5 million different apps
13 available for Apple devices. Statista, *Number of Available Apps in the Apple App Store*
14 *from July 2008 to June 2015* (2016).³⁶ These programs enable users to access a variety
15 of services and download up-to-date information.
16
17
18
19
20
21
22

23 _____
24 ³³ <http://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965#sthash.2iaYCGit.dpuf>.

25 ³⁴ <http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html>.

26 ³⁵ <http://www.business2community.com/infographics/mobile-apps-usage-statistics-trends-infographic-01248837#K6VUYPJKG1UcyiT8.99>.

27 ³⁶ <http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>.

1 *Medical Records*

2 Many users rely on their cell phones to access sensitive medical information.
3
4 Some of these applications provide complete access to medical history files that
5 include private information about health conditions and medications. The Medicare
6 Blue Button allows patients to download their medical history into a simple text file on
7 their smartphone. Medicare, *Download Claims with Medicare’s Blue Button*.³⁷ Third
8 party applications also help patients and doctors manage records and treatments online.
9 For example, Drchrono is an “integrated practice management, electronic health record
10 & medical billing platform” built for the iPad, iPhone, and Apple Watch. *drchrono*
11 (2016).³⁸ Drchrono integrates with the remote file server Box, allowing patients and
12 doctors to share files via third party servers. *drchrono, Box* (2016).³⁹ Other applications
13 allow users to log information about their fitness habits, nutritional intake, menstrual
14 cycles, blood pressure, and medication times. According to Pew Research, 19% of
15 smartphone users have a health app on their phone. Susannah Fox & Maeve Duggan,
16 *Mobile Health 2012*, PewResearch Internet Project.⁴⁰

17
18
19 Users have expressed a clear desire for privacy regarding health data. Deloitte
20 Consulting reports that 35% of survey respondents stated that they were concerned that
21 the privacy and security of their personal information might be at risk when using a
22 mobile device to access health records or tests online. Deloitte Consulting, *mHealth: a*
23 _____
24

25 _____
26 ³⁷ <https://www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html> (last visited Mar. 2, 2016).

27 ³⁸ <https://www.drchrono.com/>.

28 ³⁹ <https://www.drchrono.com/partners/box/>.

⁴⁰ <http://www.pewinternet.org/fact-sheets/health-fact-sheet/> (last visited Mar. 2, 2016).

1 *Check-up on Consumer Use* (2014).⁴¹ Apple and other device manufacturers have
2 responded to these concerns, creating new features to secure sensitive health data.

3
4 Apple. *Approach to Privacy* (2016).⁴²

5 *Messaging Services*

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

14
15
16 Mobile phones also provide access to online social networking accounts. Most
17 social networking services also offer private messaging services. Facebook, the most
18 popular service with 1.04 billion daily active users, Facebook, *Stats* (2016),⁴⁵ allows
19 users to communicate privately via an instant messaging tool and an email-like
20 messaging function, Facebook, *Managing Messages* (2016).⁴⁶ Twitter, which has 320
21 million monthly active users, 80% of which use their phone to tweet, Twitter,

22
23
24 ⁴¹ <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-chs-mhealth-infographic.pdf>.

25 ⁴² <http://www.apple.com/privacy/approach-to-privacy/>.

26 ⁴³ <http://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/>.

27 ⁴⁴ <https://support.google.com/mail/answer/1205704?hl=en>.

28 ⁴⁵ <http://newsroom.fb.com/company-info/>.

⁴⁶ <https://www.facebook.com/help/www/336759363070078/>.

1 *Company Facts* (2016),⁴⁷ allows users to publicly post text or picture messages
2 (“tweets”) or to send private, “direct messages” to other users, Twitter, *Getting Started*
3 *With Twitter* (2016).⁴⁸

4 *Photos and Videos*

5 One of the key features of the iPhone and other mobile devices is the built-in
6 photo and video camera. See Apple, *iPhone 6s Cameras* (2016).⁴⁹ These devices
7 enable users to create and store files that can include images of family members or
8 other private matters. Apple also has a built-in photo-sharing feature for iPhone users.
9 See Apple, *iCloud Photo Sharing* (2016).⁵⁰ This app allows users to create and share
10 photos with other users, and “[a]ny edits you make are automatically updated
11 everywhere.” *Id.* Users even get “real-time notifications” when someone joins an
12 album, posts a photo, or makes a comment. *Id.* This means that at any time a users
13 phone could automatically receive new private photos from their friends, without even
14 opening the app. Anyone who has access to a user’s phone could also browse or
15 download these private photos.
16
17
18

19 *Library Records*

20 Individuals increasingly use their smartphones to access books, films, music,
21 and databases available from their library, and to keep records of their library use.
22 Third-party library apps—such as Overdrive , Hoopla, Freegal, OneClickDigital, and
23 3M —allow library users to borrow or stream content and store a record of the books,
24
25

26 ⁴⁷ <https://about.twitter.com/company>.

27 ⁴⁸ <https://support.twitter.com/articles/215585>.

28 ⁴⁹ <http://www.apple.com/iphone-6s/cameras/>.

⁵⁰ <https://www.apple.com/icloud/photos/>.

1 music, and movies accessed through these apps. Over 90 libraries and library systems
2 have taken the next step and provide dedicated apps for the iPhone that integrate the
3 library’s circulation system with its public catalogs and the user's library records.
4

5 *Remote File Storage*

6 Remote file storage services allow users to store, access, edit, and share their
7 files, including word processing documents, presentations, spreadsheets, pictures,
8 music, and videos. Many of these file storage services can be accessed remotely from
9 mobile apps installed on a smartphone. These files are private and can include a great
10 deal of sensitive personal information—financial records, private messages,
11 photographs, personal notes, and health records.
12

13 *Financial Records & Transactions*

14 Consumers are increasingly pursuing services “that allow consumers to obtain
15 financial account information and conduct transactions with their financial institution
16 (‘mobile banking’) and that allow consumers to make payments, transfer money, or
17 pay for goods and services (‘mobile payments’).” Bd. of Gov’s of the Fed. Reserve
18 Sys., *Consumer and Mobile Financial Services 2015*, at 5 (Mar. 2015).⁵¹ In 2014, 39%
19 of mobile phone users and 52% of smartphone users with bank accounts used mobile
20 banking apps while 22% of mobile phone users and 28% of smartphone users used
21 mobile payment apps. *Id.* Many banks have dedicated apps that provide their
22
23
24
25
26

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

1 customers with mobile account access. *See, e.g., Bank of America, Mobile Banking*
2 (2016);⁵² Wells Fargo, *Apps* (2016);⁵³ Chase, *Mobile Banking* (2016).⁵⁴
3

4 Mobile apps also provide access to other financial data. For example, Mint is a
5 popular financial tracking app that aggregates all of a user’s financial accounts and
6 records into one place. Mint, *How it Works* (2016).⁵⁵ And transactional apps, such as
7 Uber, PayPal, and Venmo, typically store bank or credit card information, allowing for
8 automatic payments.
9

10 *Remote Desktop Clients*

11 Mobile apps even enable users to access their home computers remotely from
12 their cell phone. From these “remote desktop” apps, users can view and control their
13 desktop computers, including running programs, viewing files, and connecting to the
14 remote network. *See, e.g., Citrix, GoToMyPC* (2016).⁵⁶ This means that if a user has
15 installed the software on their home or work computer, and configured the mobile app
16 on their cell phone, anyone with access to the phone can “simply open the app,” enter
17 the user’s credentials, and be “instantly connected to” that remote computer. Citrix,
18 *GoToMyPC: Total Mobility – Factsheet* (2012).⁵⁷ These apps are especially popular
19 with employers because they can be used to “[i]ncrease employee productivity and
20 flexibility.” *Id.*
21
22

23 _____
24 ⁵² <https://www.bankofamerica.com/online-banking/mobile.go>.

25 ⁵³ <https://www.wellsfargo.com/mobile/apps/>.

26 ⁵⁴ <https://www.chase.com/online/digital/mobile-banking.html>.

27 ⁵⁵ <https://www.mint.com/how-mint-works>.

28 ⁵⁶ <https://www.citrix.com/products/gotomypc/overview.html>.

⁵⁷ http://www.gotomypc.com/remote_access/images/pdf/GoToMyPC_Mobile_App_Factsheet.pdf.

1 **B. Smartphones also serve as an authenticator and key to many sensitive**
2 **accounts and services**
3

4 Smartphones not only store and provide access to a wealth of sensitive data, they
5 also act as a key to access a user’s many accounts—social media accounts, bank
6 accounts, e-mail accounts, and other profiles. Users are typically required to create
7 unique, complex passwords for these accounts. But most people struggle to create and
8 remember strong passwords. See Troy Hunt, *The Only Secure Password is the One*
9 *You Can’t Remember*, Lifehacker (Mar. 24, 2011);⁵⁸ Phillip Inglesant & M. Angela
10 Sasse, *The True Cost of Unusable Password Policies: Password Use in the Wild*, Proc.
11 SIGCHI Conf. Hum. Factors Comp. Sys. (2010) (“We find that users are in general
12 concerned to maintain security, but that existing security policies are too inflexible to
13 match their capabilities, and the tasks and contexts in which they operate.”).⁵⁹
14
15

16 Smartphones provide an attractive solution to this problem: storing passwords
17 and other login information on the device so that the user can access protected services
18 without repeatedly entering the complex password. For example, Apple has built a
19 password storage system into the iPhone. See Apple, *Frequently Asked Questions*
20 *About iCloud Keychain* (2015) (“iCloud Keychain keeps your Safari website
21 usernames and passwords, credit card information, and Wi-Fi network information up
22 to date across all of your approved devices.”). Some mobile apps also keep users
23 logged in by default. Other apps provide storage of user login information for many
24
25

26 _____
27 ⁵⁸ <http://lifehacker.com/5785420/the-only-secure-password-is-the-one-you-cant-remember>.

28 ⁵⁹ Available at <http://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf>.

1 sites and applications in one place. This means that a user's online identities are all
2 easily accessible to anyone who has access to their phone.
3

4 Many applications have password saving features and generally, "by default,
5 applications will store your passwords and never ask you for them again." Jonathan
6 Garro, *Mac Computer Skills: Unlock the Power of Your Mac's Keychain Utility*, Tuts+
7 (Apr. 15, 2013).⁶⁰ For example, when a user logs into Facebook on their iPhone, the
8 app will keep the user logged in by default and store the password information. Some
9 social media accounts, such as Twitter and Facebook, are even embedded into the
10 phone software, requiring the user to take affirmative steps to log out. *See* Twitter,
11 *How to Sign Out of Twitter for iPhone* (2016);⁶¹ Facebook, *How Do I Log Out of The*
12 *iPhone or Ipad App?* (2016).⁶² Many users rely on these features, but the convenience
13 of automatically logging in to an app or account also makes it easier for a criminal or
14 third party to gain unauthorized access.
15
16

17 Users can also install a specific app, called a password manager, to store all of
18 their online login information. Many of these password managers are available for
19 current smartphones, including Last Pass, Onesafe, and 1Password. Kit Eaton, *Apps to*
20 *Protect Your Array of Passwords*, N.Y. Times (Oct. 17, 2013). The user enters the
21 passwords for all the websites and applications they wish to use, including banking,
22 medical, and other extremely sensitive accounts. These passwords are secured by a
23
24

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

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

27 ⁶² <https://www.facebook.com/help/iphone-app/112099682212213?rdrhc>.

1 master password. As with the in app storage of passwords, the password manager
2 provides access to sensitive accounts and data not stored on the phone.
3

4 In addition to storing passwords that provide access to a user’s online accounts,
5 smartphones also provide a mechanism to verify a user’s identity. This type of
6 authentication, commonly referred to as “two-factor authentication,” is becoming
7 standard for many online accounts. See Michelle Maisto, *Google Nudges Customers*
8 *Toward Two-Factor Authentication*, InformationWeek (Mar. 2, 2016).⁶³ The process
9 works by sending the user a unique code in a text message, or requiring the user to
10 input a code generated by an authenticating app (e.g. RSA SecureID Software Token
11 for iOS or Google Authenticator). This adds an extra layer of security for online
12 accounts, but also makes the smartphone a key target for criminals, identity thieves,
13 and intelligence agencies. See *The Encryption Tightrope: Balancing Americans’*
14 *Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 11
15 (2016) (testimony of Susan Landau, Professor, Worcester Polytechnic Institute)⁶⁴
16 (noting that “the most valuable data for attackers is your login credentials”).
17
18

19
20 **C. Smart phones enable access to a person’s home and control over the**
21 **appliances within the home**

22 Mobile phones now also provide for direct control of appliances and utilities in
23 the user’s home. Ninety-three percent of smartphone users recently expressed interest
24 in using their mobile phones to remotely control their home temperature, lights, and
25

26 ⁶³ <http://www.informationweek.com/software/productivity-collaboration-apps/google-nudges-customers-toward-two-factor-authentication/d/d-id/1324502>.

27 ⁶⁴ http://judiciary.house.gov/_cache/files/b3af6e9e-b599-4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf.

1 other utilities. Wi-Fi Alliance, *Connect Your Life: Wi-Fi and the Internet of Everything*
2 9 (2014).⁶⁵
3

4 For example, General Electric offers a range of wi-fi-connected ovens,
5 refrigerators, dishwashers, and laundry machines that users can control with mobile
6 apps. General Electric, *GE Wifi Connect* (2016).⁶⁶ Nest, recently acquired by Google,
7 has devised the Nest Thermostat, which “learns what temperature you like and builds a
8 schedule around yours.” Nest, *Meet the Nest Thermostat* (2016).⁶⁷ Other Nest products
9 include a smoke alarm that can send mobile alerts to your phone, Nest, *Meet Nest*
10 *Protect* (2016),⁶⁸ and a security camera with 24/7 live streaming and activity alerts,
11 Nest, *Meet Nest Cam* (2016).⁶⁹ The Nest App allows a user to “change the temperature
12 or view your energy usage on your Nest Thermostat, get smoke and carbon monoxide
13 alerts from your Nest Protect, watch Nest Cam video footage, and much more.” Nest,
14 *Learn More About What You Can Do With The Nest App* (July 14, 2015).⁷⁰
15
16

17 Companies have even begun offering digital door locks that can be unlocked
18 using an iPhone or other mobile device. See August, *August Smart Lock* (2015);⁷¹
19 Kwikset, *Kevo Smart Lock* (2016).⁷² Smartphones can similarly be used to deactivate a
20
21

22
23 ⁶⁵ https://www.wi-fi.org/system/files/wp_Wi-Fi_Internet_of_Things_Vision_20140110.pdf.

24 ⁶⁶ <http://www.geappliances.com/ge/connected-appliances/>.

25 ⁶⁷ <https://nest.com/thermostat/meet-nest-thermostat/?alt=3>.

26 ⁶⁸ <https://nest.com/smoke-co-alarm/meet-nest-protect/>.

27 ⁶⁹ <https://nest.com/camera/meet-nest-cam/>.

28 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>.

1 user's home security system, open their garage door, and control other home security
2 features. Livewatch, *Controlling Your Alarm System from Your Smart Phone* (2016).⁷³
3

4 * * *

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

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

12 EPIC, *Cryptography & Liberty 1999: An International Survey of Encryption Policy*
13 (1999). But it was the framers of the Constitution who first made clear that security is a
14 fundamental right of individuals. U.S. Const. amend. IV (“The right of the people to be
15 *secure* in their persons, houses, papers, and effects, against unreasonable searches and
16 seizures, shall not be violated” (emphasis added)).
17

18
19
20
21
22
23
24
25
26
27
28

⁷³ <https://www.livewatch.com/control-alarm-system-with-smartphone>.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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