

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

-----X

IN RE ORDER REQUIRING APPLE INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY  
THE COURT

Docket Nos. 15-MC-1902(JO)  
14-CR-387(MKB)

-----X

**BRIEF OF *AMICI CURIAE* FEDERAL LAW ENFORCEMENT OFFICERS  
ASSOCIATION, THE ASSOCIATION OF PROSECUTING ATTORNEYS, INC.,  
AND THE DISTRICT ATTORNEYS ASSOCIATION OF THE STATE OF NEW  
YORK IN SUPPORT OF THE GOVERNMENT'S APPLICATION FOR AN ORDER  
COMPELLING APPLE INC. TO ASSIST LAW ENFORCEMENT AGENTS IN THE  
EXECUTION OF A SEARCH WARRANT**

Joseph V. DeMarco (JD9602)  
Urvashi Sen (US2602)  
**DEVORE & DEMARCO LLP**  
99 Park Avenue, Suite 1100  
New York, New York 10016  
Phone: (212) 922-9499  
Fax: (212) 922-1799  
Email: [jvd@devoredemarco.com](mailto:jvd@devoredemarco.com)  
[usen@devoredemarco.com](mailto:usen@devoredemarco.com)

Attorneys for *Amici Curiae*

**TABLE OF CONTENTS**

Statement of Interest of *Amici Curiae*..... 1

Facts and Summary of the Argument..... 3

Argument..... 6

    I.    A Ruling in Favor of Apple Here Will Have a Chilling  
        Effect on Public Assistance to Law Enforcement ..... 6

    II.   If Apple Does Not Provide Reasonable Assistance to the  
        Government it Will Hinder Everyday Law Enforcement  
        and Endanger Public Safety ..... 10

Conclusion..... 19

**TABLE OF AUTHORITIES**

**Cases**

*Babington v. Yellow Taxi Corp.*,  
164 N.E. 726 (N.Y. 1928) ..... 6

*In re Application of U.S. for an Order Authorizing an In-Progress  
Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122  
(9th Cir. 1980)..... 8, 9

*In re Application of U.S. for an Order Directing X to Provide Access  
to Videotapes*, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003)..... 8, 9

*In re Quarles and Butler*,  
158 U.S. 532 (1895) ..... 7

*In the Matter of Search of an Apple iPhone Seized During Execution  
of a Search Warrant on a Black Lexus IS300, Cal. License  
Plate 35KGD203*, No. ED 15-0451M, 2016 WL 618401  
(C.D. Cal. Feb. 16, 2016)..... 9

*Michigan Bell Tel. Co v. United States*,  
565 F.2d 385 (6<sup>th</sup> Cir. 1977)..... 7

*Roviaro v. United States*,  
353 U.S. 53 (1957) ..... 6

*State v. Floyd*,  
584 A.2d 1157 (Conn. 1991)..... 7

*United States v. Hall*,  
583 F. Supp. 717 (E.D. Va. 1984) ..... 8, 9

*United States v. New York Telephone Co.*  
434 U.S. 159 (1977)..... 6, 9

**Statutes**

28 U.S.C. § 1651..... 8

Conn. Gen. Stat. Ann. § 53a-167b ..... 7

N.Y. Penal Law § 195.10 ..... 3, 7

Vt. Stat. Ann. T. 24 § 300-01 ..... 7

**Other Authorities**

Apple Inc., Privacy – Government Information Requests – Apple,  
<http://www.apple.com/privacy/government-information-requests/> (last visited Feb. 29, 2016) ..... 16

*The Encryption Tightrope: Balancing Americans’ Security and Privacy: Hearing Before the H. Judiciary Comm.*, 114th Cong. 6 (2016) (written testimony of Cyrus R. Vance, Jr., N.Y. County Dist. Attorney)..... 11, 12

Lori Hinnant & Karl Ritter, *Discarded Cell Phone Led to Paris Attacks Ringleader*, Associated Press, Nov. 19, 2015..... 15

NEW YORK COUNTY DISTRICT ATTORNEY’S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY’S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 9 (Nov. 18, 2015) ..... 12, 13, 14, 15, 16

NPR, *It’s Not Just The iPhone Law Enforcement Wants To Unlock*, Feb. 21, 2016, <http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock> (last visited Feb. 25, 2016)..... 5

Peter Holley, *A Locked iPhone May Be the Only Thing Standing Between Police and This Woman’s Killer*, Wash. Post, Feb. 26, 2016..... 9

**STATEMENT OF INTEREST OF *AMICI CURIAE***

The Federal Law Enforcement Officers Association (“FLEOA”), a volunteer organization founded in 1977, is the largest nonpartisan, nonprofit professional association exclusively representing federal law enforcement officers. FLEOA represents more than 26,000 uniformed and non-uniformed federal law enforcement officers from over 65 different agencies. FLEOA is a charter member of the Department of Homeland Security Federal Law Enforcement Advisory Board, holds two seats on the Congressional Badge of Bravery Federal Board, and serves on the Executive Board of the National Law Enforcement Officers Memorial Fund and the National Law Enforcement Steering Committee. FLEOA provides a legislative voice for the federal law enforcement community and monitors legislative and other legal issues that may impact federal law enforcement officers.

The Association of Prosecuting Attorneys, Inc. (“APA”) is a national not-for-profit organization headquartered in Washington, D.C. and made up of elected and appointed prosecuting attorneys from throughout the nation. The APA provides valuable resources such as training and technical assistance to prosecutors in an effort to develop proactive and innovative prosecutorial practices that prevent crime, ensure equal justice, and help make our communities safer. The APA also acts as a global forum for the exchange of ideas, allowing prosecutors to collaborate with all criminal justice partners, providing timely and effective technical assistance as well as access to technology for the enhancement of the prosecutorial function. The APA serves as an advocate for prosecutors on emerging issues related to the administration of justice and development of partnerships.

The District Attorneys Association of the State of New York (“DAASNY”), currently led by Rockland County District Attorney Thomas P. Zugibe, is a statewide organization composed of elected county District Attorneys from throughout New York State, as well as assistant district attorneys, a membership body with about approximately 2,500 prosecutors. Members of DAASNY are from some of the largest prosecutorial offices in the United States, such as New York County, that employs hundreds of prosecutors, to the smallest, with perhaps only a single prosecutor. In their work as prosecutors, DAASNY members continually confront how best to exercise their advocacy function in fulfilling their duties.

*Amici* and their members are called upon on a daily basis to protect and serve the public by investigating criminal activity and wrongdoing and ensuring that the individuals responsible for it pay the penalty for their crimes. In order to fulfill their duties, *Amici* members must have access to all reasonable means of procuring relevant evidence. In this digital age, data stored on mobile devices has proven, time and time again, to be critical in assisting law enforcement officers to do their jobs. *Amici* and their members thus have a strong interest in ensuring that the Government’s Application is granted.

## FACTS AND SUMMARY OF THE ARGUMENT

For centuries, citizens have been required to provide reasonable assistance to law enforcement. This was true at common law in ancient England. It was true in Colonial America. And it was true even as new technologies -- from automobiles and telephones to credit cards and recording devices -- transformed American society. It remains true today.

The failure to provide “reasonable assistance” may even be criminalized. For example, under New York’s Penal Law, “[a] person is guilty of refusing to aid a peace or a police officer when, upon command by a peace or a police officer identifiable or identified to him as such, he unreasonably fails or refuses to aid such peace or a police officer in effecting an arrest, or in preventing the commission by another person of any offense.” N.Y. Penal Law § 195.10. This is black letter law, not just in New York State, but in other states which have enacted similar laws requiring ordinary citizens -- rich or poor, weak or strong -- to reasonably assist law enforcement in carrying out their mandates to keep the peace and to maintain law and order.

For years, Apple Inc. (“Apple”) has followed this well-settled mandate, and, in doing so, has been a valuable partner to *Amici*. Apple managers have discharged their responsibilities as citizens to provide reasonable assistance to law enforcement executing search warrants and other court orders. Consistent with that long-standing practice, Apple in this case initially agreed to help the government execute a court-ordered search warrant by unlocking an Apple iPhone 5s running iOS 7 that a criminal had been using to further a methamphetamine drug distribution conspiracy.<sup>1</sup> Apple even helped the government to craft the proposed language for the order directing it to work with the government.<sup>2</sup> However,

---

<sup>1</sup> *In re Apple, Inc.*, No. 15-MC-1902 (JO), 2016 WL 783565, at \*2-4 (E.D.N.Y. Feb. 29, 2016).

Apple changed its position when United States Magistrate Judge Orenstein called upon it to comment on the applicability of the All Writs Act to this case. Apple suddenly opposed the government's application, declaring the government's request "unreasonable." Unfortunately, Judge Orenstein agreed with Apple's new view and, in a February 29, 2016 Order (the "Orenstein Order") denied the government's application for an order requiring Apple to effect a passcode bypass and extract data from the criminal's iPhone.<sup>3</sup>

*Amici* are surprised and disappointed in Apple's position. Apple has decided not to help the government even though: (1) Apple has assisted the government in accessing data on locked Apple devices literally *dozens* of times before;<sup>4</sup> (2) Apple, by its own admission, has "on the shelf" technology to help the government search the iPhone in this case and therefore would not need to write new computer code to do so;<sup>5</sup> and (3) as a result, Apple will not be substantially burdened by helping the government.<sup>6</sup>

---

<sup>2</sup> *Id.* at \*2-3.

<sup>3</sup> *Id.* at \*1.

<sup>4</sup> The Government's Memorandum Of Law In Support Of Its Application For An Order Compelling Apple Inc. To Assist Law Enforcement Agents In The Execution Of A Search Warrant at 17, *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, No. 15-MC-01902 (MKB), Dkt. 30 (E.D.N.Y. Mar. 7, 2016).

<sup>5</sup> Apple Inc.'s Memorandum Of Law In Response To The Government's Brief In Support Of Its Application For An Order Compelling Apple Inc. To Assist Law Enforcement Agents In The Execution Of A Search Warrant at 5, *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, No. 15-MC-01902 (MKB), Dkt. 40 (E.D.N.Y. Apr. 15, 2016) ("Apple's Brief").

<sup>6</sup> *See id.*

On March 7, 2016, the government filed an application before this Court for an order compelling Apple's assistance in this matter (the "Government's Application").<sup>7</sup> *Amici* respectfully submit this brief in support of the Government's Application.

*Amici* believe that the position that Apple has taken, and that the Magistrate Judge adopted, is a dangerous one. *First*, if Apple were to prevail in this Court, the public at large may think twice about cooperating with law enforcement when called upon to do so, invalidating centuries of well-settled law and common practice. *Second*, Apple's refusal to provide assistance, if validated by this Court, will have far-reaching public safety ramifications by giving criminals a safe haven to conduct their unlawful activities, while concomitantly making it more difficult -- and in some cases impossible -- for law enforcement to fulfill its obligation to investigate crimes, protect the public by bringing criminals to justice, and enforce the law. In short, on these facts, *Amici* are hard-pressed to find a situation in which it would be *more* reasonable for the government to request Apple's assistance, and for this Court to approve such a request.

---

<sup>7</sup> The Government's Memorandum Of Law In Support Of Its Application For An Order Compelling Apple Inc. To Assist Law Enforcement Agents In The Execution Of A Search Warrant, *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, No. 15-MC-01902 (MKB), Dkt. 30 (E.D.N.Y. Mar. 7, 2016).



## ARGUMENT

### I. A RULING IN FAVOR OF APPLE HERE WILL HAVE A CHILLING EFFECT ON PUBLIC ASSISTANCE TO LAW ENFORCEMENT

For centuries, it has been the law that the citizenry are required to provide law enforcement with reasonable assistance in the apprehension of criminals and the investigation of crimes. This was true at common law in medieval England. It was true in the fledgling Colonies. It was true as new technologies transformed American culture and society. It remains true today.

In *Babington v. Yellow Taxi Corporation*, a police officer, pursuing a car containing suspected thieves, hopped onto a taxi cab running board and ordered the cab driver to chase the car. *See* 164 N.E. 726 (N.Y. 1928). During the chase, the cab driver was killed in an accident with a “touring car”. Insurance and worker’s compensation litigation followed. During the litigation, the courts were confronted with whether the cab driver was lawfully required to participate in the officer’s pursuit of the suspects. Writing for the Court of Appeals, New York’s highest court, Judge Benjamin Cardozo held that the cab driver *was* duty-bound to follow the officer’s instructions. Examining the historic nature of that duty, Cardozo stated: “[A]s in the days of Edward I [King of England], the citizenry may be called upon to enforce the justice of the state, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand.” *Id.* at 727. Judge Cardozo also opined for the Court that this historic duty was not nullified by new technology, including, in that case, the mass-produced automobile (then around 20 years old): Although “[t]he horse has yielded to the motorcar as an instrument of pursuit and flight,” the “ancient ordinance abides as an interpreter of the present duty.” *Id.*

Almost 50 years later, Justice White echoed Judge Cardozo’s words in a case involving another new technology in the Supreme Court’s landmark decision, *United States v. New York Telephone Co.*, confirming once more that “citizens have a *duty* to assist in enforcement of the laws.” 434 U.S. 159, 175 n.24 (1977) (emphasis added); *see also*

*Roviaro v. United States*, 353 U.S. 53, 59 (1957) (recognizing the historic obligation of citizens to assist law enforcement and to communicate their knowledge of criminal activity to law enforcement officials); *In re Quarles and Butler*, 158 U.S. 532, 535 (1895) (recognizing the duty of citizens “to assist in prosecuting, and securing the punishment of, any breach of the peace of the United States”). Indeed, as Connecticut’s highest court has recognized:

The basic concept that every citizen can be compelled to assist in the pursuit or apprehension of suspected criminals has ancient Saxon origins, predating the Norman Conquest . . . . As the responsibility for keeping the peace shifted, over the centuries, to sheriffs, constables, and eventually to trained professional police departments, the power of those law enforcement officials to command the assistance of citizens was recognized both in statutes and in the common law.

*State v. Floyd* (“*Floyd*”), 584 A.2d 1157, 1166 (Conn. 1991) (unanimously upholding state statute requiring citizens to provide reasonable assistance to law enforcement in case involving factory security guards who refused to come to assistance of police officer during officer’s altercation with factory employee) (internal citations omitted) (footnotes omitted); *see also Michigan Bell Tel. Co v. United States*, 565 F.2d 385, 389 (6<sup>th</sup> Cir. 1977) (recognizing that at common law a sheriff could require even unwilling citizens to “assist him in executing the king’s writs, effecting an arrest, quelling riots and apprehending robbers”).<sup>8</sup>

---

<sup>8</sup> *See also* N.Y. Penal Law § 195.10 (a person is guilty of a class B misdemeanor for “unreasonably fail[ing] or refus[ing] to aid” a “peace or a police officer in effecting an arrest, or in preventing the commission by another person of any offense” when commanded to do so); Conn. Gen. Stat. Ann. § 53a-167b (a person is guilty of a class A misdemeanor for “failure to assist a peace officer, special policeman, motor vehicle inspector or firefighter” when commanded to do so); Vt. Stat. Ann. T. 24 § 300-01 (imposing fines and, under certain circumstances, imprisonment for failure to assist a “sheriff or other officer in the discharge of the duties of his office, for the preservation of the peace, or the suppression or prevention of an criminal matter or cause”).

Nor is this principle some dusty, historical relic, applied only to sepia-colored fact patterns. To the contrary, reasonable assistance has been required of third parties in cases involving technologies that were once as novel as smartphones, including: telephones as noted above, *see also In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities* (“*Mountain Bell*”), 616 F.2d 1122, 1132 (9th Cir. 1980); credit cards, *see United States v. Hall*, 583 F. Supp. 717, 720-21 (E.D. Va. 1984); and video recordings and video tapes, *see In re Application of U.S. for an Order Directing X to Provide Access to Videotapes* (“*Videotapes*”), No. 03-89, 2003 WL 22053105, at \*1-2 (D. Md. Aug. 22, 2003).<sup>9</sup>

The reasons supporting continued application of this venerable principle are clear. *Especially* in this digital age, where information used by criminals can be transmitted around the globe at the speed of light and secured thorough robust encryption, it is critical for public safety that technology companies and the citizens who manage them reasonably to cooperate with law enforcement. As the cases above demonstrate -- and as Cardozo foresaw -- this is not the first nor the last time that law enforcement enlists the assistance of citizen-managers of corporations to help them ensure that the law, the bedrock of our society, is followed; that “the ancient ordinance” is applied to current technology; and that our officers and prosecutors have the tools and information necessary to enforce law, prevent crime, and protect the citizenry.

---

<sup>9</sup> Apple asserts that these cases are distinguishable because the “res” subject to third party assistance in those cases was in the possession of the third party at the time assistance was requested, whereas in this case the iPhone at issue is not (yet) Apple’s possession. *See* Apple’s Brief, at 19-20. But this is a distinction without a difference, for the touchstone of what is (or is not) reasonable assistance required under the All Writs Act does not depend on who has possession of the property that is the subject of the assistance, and *Amici* are aware of no case where physical possession of the property has been dispositive of what is required of a third party under the All Writs Act.

In *New York Telephone Co.*, the Supreme Court used the authority of the All Writs Act, 28 U.S.C. § 1651(a), to order the phone company to do what it was plainly able to do to assist the FBI in using the company's facilities and equipment to apprehend a group suspected of illegal gambling. See 434 U.S. at 172, 17; see also *Mountain Bell*, 616 F.2d at 1132. Other courts in other cases involving other crimes and other technologies have reached similar results. See *Hall*, 583 F. Supp. at 720-21; *Videotapes*, 2003 WL 22053105, at \*2-3.<sup>10</sup> *Amici* respectfully submit that this Court, too, should rely upon this case law and use the All Writs Act to order Apple to do what it is plainly and reasonably able to do -- utilize its already-existing technology to assist law enforcement by performing a passcode bypass to retrieve data from a cell phone a criminal co-conspirator used to further his crimes.<sup>11</sup>

In short, law enforcement's request here is, in principle, neither new nor novel. What *is* new is Apple's sudden refusal to assist law enforcement with a very reasonable

---

<sup>10</sup> It bears noting that the request here is even less intrusive than was the case in *New York Telephone Co.* Here, the data at issue is "at rest," static data that exists on a phone. In *New York Telephone Co.*, the data that was to be accessed was wiretap data belonging to a group of illegal gamblers who were unaware that the most private details of their phone conversations were being intercepted real-time by law enforcement. And it goes without saying that the government's request of Apple is orders of magnitude less than what was required of either cab driver William Babington or the security guards in *Floyd*.

<sup>11</sup> On February 16, 2016, a United States Magistrate Judge in California found that the All Writs Act gave it the authority to order a similar search of an iPhone used by a terrorist in the deadly shootings at San Bernardino, California on December 2, 2015. See Order Compelling Apple, Inc. To Assist Agents in Search, *In the Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203*, No. ED 15-0451M, 2016 WL 618401, at \*1 (C.D. Cal. Feb. 16, 2016). This was in spite of the fact that the iPhone in question in that case was actually running a more advanced version of iOS and Apple claimed not to have the technology to unlock that iPhone. That is not the case here, where Apple essentially has "stock" procedures and "off the shelf" technology that it can use to provide the government with the assistance it has requested.

request, one that they have complied with numerous times in the past. *Amici* are concerned that were Apple's new position to prevail in this case, the public at large may question the "ancient ordinance" and hesitate when called upon to cooperate with law enforcement. In countless ways -- both knowable and unknowable -- this will hamper *Amici's* ability to detect, deter, and punish crime.

**II. IF APPLE DOES NOT PROVIDE REASONABLE ASSISTANCE TO THE GOVERNMENT IT WILL HINDER EVERYDAY LAW ENFORCEMENT AND ENDANGER PUBLIC SAFETY**

The government has represented to the Court that it needs to search the iPhone Jun Feng ("Feng") used while committing his crimes, particularly given that those crimes likely involved unapprehended co-conspirators. Yet beyond the facts of this crime, a ruling that validates Apple's position can only serve to hamper *Amici's* ability to bring criminals to justice and justice to victims. To be clear: if the Court adopts Apple's reasoning, public safety *will* suffer. Crimes *will* go unsolved and criminals *will* go free. Apple's iPhones and iPads are ubiquitous. They are powerful and are growing more powerful with each new generation. They are used by criminals, as well as crime victims. And, until recently, Apple was willing to assist law enforcement in executing court orders to search these devices. But Apple has changed course. In this case it has refused to assist in the search of phones it plainly can. Moreover, it continues to redesign its iOS operating system to make its products far harder, or indeed impossible, to search, even where law enforcement provide sufficient probable cause to allow a neutral magistrate to issue a search warrant. These decisions -- decisions by citizens -- are already impeding and damaging law enforcement investigations nationwide. As law enforcement officials who are sworn to ensure public safety, and to solve crimes, *Amici* are the first responders, the investigators, the law

enforcers and the prosecutors who, day-in and day-out, must live with Apple's decisions. To *Amici*, this is *not* a theoretical debate. It is as real as a drug dealer gone free, as real as a pedophile planning for his next prey, as real as a terrorist plotting the destruction of innocent life.

The importance of access to evidence found on iPhones, iPads, and similar devices is emphasized by actual, real world examples Apple cannot dispute. For example, in the Manhattan District Attorney's office *approximately 50%* of the mobile devices currently recovered during investigations are inaccessible to law enforcement because they run Apple's newer operating systems.<sup>12</sup> As the District Attorney in Manhattan put it:

In some cases, we can't move at all. We can't establish liability or responsibility because we can't access the phone. In others, it's affecting our ability to gather all the evidence that's needed to make sure that we are making the right judgments. And I think it's very important for people to understand that a prosecutor's job is to investigate, get all the information and then make the right judgment as to whether or not we can go forward. It's also our responsibility to make sure that we are prosecuting the right people. And when we don't have access to digital devices, we don't have all the information that we need to make the best judgment as to how the case should be handled.<sup>13</sup>

Other district attorneys throughout New York State and throughout the country have had alarmingly similar experiences with iPhones running the current operating system. For example, last year the Harris County (Texas) District Attorney's Office was unable to search more than 100 encrypted (and therefore inaccessible) Apple devices from cases to date,

---

<sup>12</sup> See *The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Judiciary Comm.*, 114th Cong. 6 (2016) (written testimony of Cyrus R. Vance, Jr., N.Y. County Dist. Attorney) ("Vance Hearing Testimony"), at 6.

<sup>13</sup> NPR, *It's Not Just The iPhone Law Enforcement Wants To Unlock*, Feb. 21, 2016, <http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock> (last visited Feb. 25, 2016).

including human trafficking, violent street crimes, and sexual assaults. In 2016, the number of inaccessible Apple devices for that office already numbers eight to ten *per month*. Similarly, in January and February of this year, the Cook County (Chicago) State Attorney's office has received 30 encrypted devices it could not access, and the Connecticut Division of Scientific Services has encountered 46 encrypted Apple devices in criminal cases, including cases involving child pornography.<sup>14</sup> Even a county as small as Rockland County in New York averages about one inaccessible phone per month. These numbers will, of course, only continue to multiply as time goes on and newer Apple devices replace older ones.

Actual, real-world cases provide a window into the types of cases at stake for *Amici*:

- **Homicide (conviction of guilty)**: *People v. Hayes*<sup>15</sup>: The victim was filming a video using his iPhone when he was shot and killed by the defendant. Because the iPhone was not passcode-locked, the video, which captured the shooting, was recovered and admitted into evidence at trial. The defendant was convicted of murder and sentenced to 35 years to life.<sup>16</sup>
- **Homicide (exoneration of innocent)**: *People v. Rosario*<sup>17</sup>: A detective obtained a search warrant and an unlock order for certain iPhones found at the scene of a homicide. He sent the phones to Apple, which assisted in extracting data from them. The phone data demonstrated inaccuracies in

---

<sup>14</sup> See Vance Hearing Testimony at 6-7.

<sup>15</sup> Indictment Number 4451/12.

<sup>16</sup> NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 9 (Nov. 18, 2015), <http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf> (the "NY DA's Report").

<sup>17</sup> Indictment Number 1859/10.

what investigators initially thought to be the timeline of events, and demonstrated that a particular suspect was not, in fact, involved in the murder. A phone number stored in one of the iPhones was eventually linked to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 1/2 years' imprisonment.<sup>18</sup>

- **Child Pornography:** *People v. Hirji*<sup>19</sup>: The defendant was arrested after telling a taxi driver about his interest in having sex with children and showing the driver a child pornography image. Upon searching the defendant's iPhone pursuant to a search warrant, investigators discovered a large number of child pornography images. The defendant was convicted of Promoting a Sexual Performance by a Child.<sup>20</sup>
- **Sex Trafficking:** *People v. Brown*<sup>21</sup>: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from defendant's electronic devices contained (a) photographs showing him posing his victims for online prostitution advertisements and showing that he had "branded" multiple women with his nickname; and (b) text messages between him and several victims confirming that he had engaged in acts of violence against the

---

<sup>18</sup> NY DA's Report at 11.

<sup>19</sup> Supreme Court Information Number 3650/15.

<sup>20</sup> NY DA's Report at 9-10.

<sup>21</sup> Indictment Numbers 865/12, 3908/12, and 3338/13.



testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison.<sup>22</sup>

- **Cybercrime and Identity Theft:** *People v. Jacas et al.*<sup>23</sup> and *People v. Brahms et al.*<sup>24</sup>: An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping the credit cards through a card reader that stored the credit card number and other data. When the phone was searched pursuant to a warrant, law enforcement officials discovered text messages between the waiter and other members of the group regarding the ring's crimes. Based in large part on information obtained from the phone, investigators were able to obtain an eavesdropping warrant, and ultimately arrested a 29-member identity theft ring, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group stole 100 American Express credit card numbers and property worth over \$1,000,000. All of the defendants pled guilty, and more than \$1,000,000 in cash and merchandise was seized and forfeited.<sup>25</sup>

---

<sup>22</sup> NY DA's Report at 9.

<sup>23</sup> Indictment Number 42/12.

<sup>24</sup> Indictment Number 5151/11.

<sup>25</sup> NY DA's Report at 10-11.

- **Unlawful Surveillance:** *People v. Lema*<sup>26</sup>: The defendant was arrested for unlawful surveillance after a police officer observed the defendant using his phone to film up women’s skirts (*i.e.*, “upskirting”). The defendant consented to a search of his phone, but the passcode he provided did not work. Investigators obtained a search warrant and unlock order for the phone. The phone was sent to Apple, Apple extracted data from the phone, and the phone and data were returned to the prosecutor. Two “upskirting” videos were found on the phone, both filmed on the date of the defendant’s arrest. Following the trial, at which both videos were entered into evidence, the defendant was convicted as charged, of two counts of unlawful surveillance.<sup>27</sup>

Finally, in one current investigation in Louisiana, a locked iPhone’s text messages and other information on the device may hold the only clues to the murder of a pregnant woman gunned down at the front door of her home.<sup>28</sup> These examples, and many more, prove just how essential evidence recovered from iPhones can be.<sup>29</sup>

Of course, if Apple can refuse to assist law enforcement, it will hamper not only prosecutions, but also crime and terrorism *prevention*. Data successfully retrieved from a

---

<sup>26</sup> Indictment Number 4117/13.

<sup>27</sup> NY DA’s Report at 11.

<sup>28</sup> See Peter Holley, *A Locked iPhone May Be the Only Thing Standing Between Police and This Woman’s Killer*, Wash. Post, Feb. 26, 2016, available at <https://www.washingtonpost.com/news/post-nation/wp/2016/02/26/a-locked-iphone-may-be-the-only-thing-standing-between-police-and-this-womans-killer/>.

<sup>29</sup> *Amici* have additional specific, law-enforcement sensitive examples which it does not wish to place in the public domain. Should the Court, however, desire this information, *Amici* will make it available.

cell phone after the November 2015 Paris terrorist attacks on the Bataclan concert hall, where 89 people were killed, reportedly allowed French law enforcement officials to track down the alleged ringleader, who later died in a police raid.<sup>30</sup> This individual was in the process of planning yet another attack in Europe, and that cell phone access likely saved numerous innocent lives. Lest there be any doubt about the “value-add” for criminals by Apple’s present litigation posture compounded by its recent engineering decisions, *Amici* are even aware of jailhouse statements by criminals about how Apple’s newer iOS encryption is a helpful “feature” for planning and committing crimes. For example, in 2015, the New York Department of Corrections intercepted a phone call between an inmate and a friend about Apple’s new, impregnable operating system, during which the inmate stated: “*If our phone is running on the iOS 8 software, they can’t open my phone. That might be another gift from God.*”<sup>31</sup> In fact, *Amici* are aware of numerous instances in which criminals who previously used one time, so-called “throwaway” or “burner” phones, have now switched to newer model iPhones as the “device-of-choice” for their criminal wrongdoing.<sup>32</sup>

---

<sup>30</sup> Lori Hinnant & Karl Ritter, *Discarded Cell Phone Led to Paris Attacks Ringleader*, Associated Press, Nov. 19, 2015, available at <http://bigstory.ap.org/article/47e613d2ad184fe4802fd76de903d4bb/french-leader-extremists-may-strike-chemical-bio-arms>.

<sup>31</sup> NY DA’s Report at 12 (emphasis added).

<sup>32</sup> Apple even advertises and promotes its alleged inability to help law enforcement search its newer devices. Specifically, Apple’s website states, “On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user’s passcode, which Apple does not possess.” Apple Inc., Privacy – Government Information Requests – Apple, <http://www.apple.com/privacy/government-information-requests/> (last visited April 15, 2016).

As noted above, Apple has greatly assisted law enforcement in the past, routinely helping officers to unlock the very phones it is now stating it would offend privacy to help search.<sup>33</sup> This assistance has been critical in a number of law enforcement cases, both to prosecute criminals and to exonerate the innocent. In this case, the government has represented that it has no reasonable alternate means of obtaining the information they are seeking,<sup>34</sup> and the iPhone used by defendant Feng may well be as critical to uncovering the details and co-conspirators in this drug ring as the devices were in the cases described above. Further, the phone here runs a previous version of Apple's operating system -- iOS 7 -- and, by Apple's own admission, it would be minimally burdensome for Apple to assist in unlocking it using already-existing technology. As Apple has conceded, it "does have the technical ability to extract unencrypted user data from a locked device running iOS 7 or earlier" and it has done so on numerous occasions in the past in response to court orders.<sup>35</sup> So routine and ministerial is Apple's assistance that it initially agreed to assist law

---

<sup>33</sup> See Government's Application at 17 (noting that the All Writs Act has been used to order Apple to provide similar technical assistance to the government on 83 prior occasions); see also Apple's Brief at 5 (stating that "Apple has in the past extracted unencrypted data from locked devices running iOS 7 or earlier and provided such data to the government in response to court orders").

<sup>34</sup> See Government's Application at 41, 43 (describing how the government's ability to bypass the passcode of a locked iPhone without risking permanent inaccessibility of the evidence depends on the specific iPhone's hardware and software). Moreover, when an iPhone is locked, it is not apparent whether or not the user has activated the device's auto-erase feature, which renders the data permanently inaccessible after multiple failed passcode attempts. *Id.* at 3. Lastly, the contents of this iPhone were not backed up onto Apple's iCloud storage service, which might have otherwise provided an alternative means of obtaining at least some of the data on the iPhone. *Id.* at 4.

<sup>35</sup> Apple's Brief at 5.

enforcement when this matter was brought to Apple's attention, even going so far as to craft the language Apple required the proposed court order to include.<sup>36</sup>

In sum, it is crystal clear that Apple's refusal to provide reasonable assistance to law enforcement, if validated by this Court, will have real-world, on-the-ground implications for federal and state law enforcement officers as they do their daily jobs as well as for the public they are sworn to protect. In many instances, this assistance is critical to whether or not law enforcement can bring justice and closure to victims' families and, in cases such as this one, thwart the kind of dangerous criminal activity that poses significant threats to our neighborhoods and to our communities.

---

<sup>36</sup> See Orenstein Order at \*2-3.

## CONCLUSION

*Amici* agree with the Parties that this is an important case. It implicates privacy. It implicates security. For many years, Apple has provided crucial and commendable assistance to law enforcement. It has been a valuable partner to *Amici* in case after case. Apple has changed course in a single but potentially crucial way. Despite the Government obtaining a lawful order to search the phone in this case, Apple now refuses to assist despite its proven ability to do so. Apple is a business. And, understandably, it has represented that it has business imperatives for its decision to refuse to help the government.<sup>37</sup> If this Court upholds this refusal to assist, however, the effects of its refusal will be truly devastating for countless Americans.

DATED: April 21, 2016  
New York, NY

Respectfully Submitted,

By: /s/ Joseph V. DeMarco  
Joseph V. DeMarco (JD9602)\*  
Urvashi Sen (US2602)  
DEVORE & DEMARCO LLP  
99 Park Avenue, Suite 1100  
New York, New York 10016

Attorneys for *Amici Curiae*

\*Counsel for *amici curiae* wish to thank Law Clerk Eric G. Rosenberg for his special assistance in preparing this brief.

---

<sup>37</sup> Apple Inc.'s Response To Court Oct. 9, 2015 Memorandum And Order at 4, *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, No. 15-MC-01902 (JO), Dkt. 11 (E.D.N.Y. Oct. 19, 2015).