COPY

Stephen G. Larson (SBN: 145225)
slarson@larsonobrienlaw.com
Jerry A. Behnke (SBN: 180462)
jbehnke@larsonobrienlaw.com
Steven A. Haskins (SBN: 238865)
shaskins@larsonobrienlaw.com
Melissa A. Meister (SBN: 296744)
mmeister@larsonobrienlaw.com
LARSON O'BRIEN LLP
555 S. Flower Street, Suite 4400
Los Angeles, CA 90071
Telephone: (213) 436-4888
Facsimile: (213) 623-2000

Attorneys for **AMICUS CURIAE**
GREG CLAYBORN, JAMES GODOY,
HAL HOUSER, TINA MEINS, MARK
SANDEFUR, AND ROBERT VELASCO

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

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	Case No. 5:16-CM-00010 (SP) ***AMICUS CURIAE* BRIEF OF GREG CLAYBORN, JAMES GODOY, HAL HOUSER, TINA MEINS, MARK SANDEFUR, AND ROBERT VELASCO** Assigned to: The Hon. Sheri Pym

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Amici curiae are close relatives of those killed by a terrorist attack on a holiday party hosted by the County of San Bernardino's Department of Public Health. The terrorists murdered 14 citizens and severely injured dozens more—the worst terrorist attack on American soil since September 11, 2001. While this crime has had undeniable implications for the nation and its security, *amici* have more personal and pressing concerns—they want and need to know if they were purposefully targeted, if others in their community aided and abetted the crime, and if additional attacks targeting them or their loved ones are forthcoming.

After the attack, federal law enforcement authorities obtained warrants from a neutral magistrate to search the residence of, and vehicles used by, terrorists Syed Rizwan Farook and Tashfeen Malik. While executing a search warrant on Farook's vehicle, authorities seized an iPhone 5c belonging to the County, but used by Farook. The County gave federal authorities and Apple consent to search the phone, but the iPhone was locked. The phone's data is thus inaccessible without entering a 4- or 6-digit PIN code that investigators, unfortunately, do not have.

No one knows with certainty what unique data resides on the iPhone, but there is reason to believe it contains communications between Farook and victims, survivors, and affected loved ones of the shooting, who were Farook's coworkers. It may contain data that will help law enforcement mitigate ongoing threats. It may yield new leads or information on the completed crime, including potential co-conspirators. It may explain the motive for this senseless tragedy. And it may, if nothing else, give some measure of closure to the survivors and families of loved ones who have suffered every day since this terrible crime occurred. *Amici* are eager that no stone be left unturned in investigating this horrible act, not least because doing so may avert other tragedies and spare other citizens from the same heartbreak that victims of this crime continue to suffer.

These concerns are heartfelt and personal. They have been expressed poignantly in a letter to Apple CEO Tim Cook by one of the *amici*, Mark Sandefur, father to shooting victim Larry Daniel Eugene Kaufman:[1]

> Our son, Larry Daniel Eugene Kaufman, was one of the fourteen people killed in the terrorist shooting in San Bernardino. Daniel worked as an instructor, teaching people with disabilities the skills necessary to live independent lives. He was not what one would think of as a terrorist target of the Islamic State. . . .
>
> I have attended private briefings that are held for the families of the victims. At these briefings, we learn first-hand what the public eventually learns. We are not privy to anything *only* the FBI knows, but we talk amongst ourselves about the horrors of that day. Some of the survivors come to these meetings pushing walkers, or limping with canes. They are reminders to me of what they went through. We who lost our family members are reminders to them that it could have been worse. Several of the survivors tell me bone-chilling stories of where they were, and what they saw. Some of them describe in precise detail, laying on the floor, hiding under furniture and the bodies of their co-workers, that they saw *three* assailants, not two, walking around in heavy boots as they carried out their murders. . . .
>
> Recovery of information from the iPhone in question may not lead to anything new. But, what if there is evidence pointing to a third shooter? What if it leads to an unknown terrorist cell? What if others are attacked, and you and I did nothing to prevent it? . . .

Mr. Sandefur expresses, perhaps like no one else outside of *amici* and those touched by this tragedy, the true stakes of this dispute.

---

[1] Mr. Sandefur's letter is reproduced in its entirety as Exhibit 1.

Of course, *amici* share the concern of citizens wary of intrusion into the intimate details of their lives. Smartphones, which have become 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," allow persons to keep on their phone "a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2484, 2490 (2014). The capacity for smartphones to store a person's most personal data—their communications, finances, health information, photographs, and geolocation history—is precisely why the Supreme Court has held that law enforcement may not search a smartphone without a valid search warrant: "Our answer to the question of what police must do before searching a cell phone seized . . . is accordingly simple—get a warrant." *Id.* at 2495. Apple's refusal to aid authorities in unlocking this iPhone, however, makes the Supreme Court's simple answer much more complicated.

Apple has defended its stance by invoking the public's right to privacy, but that is not what this case is about. There is no privacy right to be enforced here, by this Court. This case is about the United States' ability to successfully execute a search warrant, obtained through adherence to the constraints of the Fourth Amendment, on an iPhone used by a terrorist. The public, and the victims of this crime, have a strong right and interest in the United States' investigation and Apple's reasonable assistance in the investigation is warranted.

Broader questions about the fate of smartphone encryption and data privacy can be saved for another day and another forum. Federal law enforcement authorities have not requested that Apple create a "backdoor" to its iPhones, allow wholesale government access to iPhones, or provide vast stores of data compiled from the records of American citizens. The United States has asked for Apple's assistance to unlock a single iPhone in the United States' lawful possession. Given

the circumstances of this case, it is reasonable to require Apple's assistance in retrieving the data on the phone.

ANALYSIS

I. This Case is Not About Privacy

This case has triggered an avalanche of commentary about its global implications. Before filing its motion for relief, Apple first took its case to the media by releasing a public letter warning of disastrous consequences should Apple be forced to assist in this investigation: "If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data." (Ex. 2.) Apple's parade of horribles continued: "The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge." (*Id.*) The media has taken up Apple's theme that this case is about the collision of personal privacy concerns and national security.[2]

But this far overstates the scope of the United States' request. This case poses no threat to individual privacy rights, and indeed, involves no intrusion to any cognizable privacy right at all. The iPhone was seized pursuant to a lawful search warrant issued by a neutral and detached magistrate. *See, e.g.*, *Johnson v. United States*, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent."). In cases where a search warrant

---

[2] *See, e.g.*, Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), *http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html*; Tony Romm & Tim Starks, *Privacy Debate Explodes Over Apple's Defiance*, POLITICO (Feb. 17, 2016), http://www.politico.com/story/2016/02/apple-iphone-san-bernardino-fbi-defiance-219394.

is lawfully issued, the right to privacy ***always*** yields to appropriate governmental authority. Under our system of laws, one does not enjoy the privacy to commit crime. *See, e.g.*, *Virginia v. Moore*, 553 U.S. 164, 171 (2008) ("[W]hen an officer has probable cause to believe a person committed even a minor crime . . . the balancing of private and public interests is not in doubt."); *Kolender v. Lawson*, 461 U.S. 352, 369 n.7 (1983) ("When law enforcement officers have probable cause to believe that a person has committed a crime, the balance of interests between the State and the individual shifts significantly, so that the individual may be forced to tolerate restrictions on liberty and invasions of privacy that possibly will never be redressed, even if charges are dismissed or the individual is acquitted.")

Additionally, there is no privacy interest implicated here because the lawful owner of the phone—the County—consents to, and actively desires, the United States' search of the iPhone. *See Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990) (finding that the Fourth Amendment's prohibition against warrantless searches and seizures does not apply "to situations in which voluntary consent has been obtained"); *see also City of Ontario v. Quon*, 560 U.S. 746, 762 (2010) (holding that government employers can search cellular phones for a "noninvestigatory, work-related purpose" or investigation of "work-related misconduct"). After stripping Apple's hyperbole about the evils of government overreach, this case's facts are nearly identical to the owner of a computer operating system losing the password for the system and calling technical support to get the password changed or reinstalling the operating system. While Microsoft and Apple routinely help

computer owners with this all-too-common situation,[3] Apple refuses to do the same in a case with national-security implications.[4]

Indeed, the mere fact that County owns the iPhone in this case distinguishes it from other cases in which authorities might seek access to an iPhone. (*See* Apple Br. at 24.) It is certainly rare that *both* law enforcement *and* an iPhone's owner have requested that Apple unlock the device. Apple's refusal to assist in this case has nothing to do with any viable privacy concern.

II. The United States' Request is Modest in Scope

The absence of a cognizable privacy interest here has not stopped Apple from taking the position that the United States' request will cause a parade of privacy horribles, culminating in the end of technological security. (Ex. A.) Nothing could be further from reality. Apple is conflating many different policy debates for the dual purposes of excusing itself from compliance with current law and protecting its public image. Certainly, debates regarding privacy, encryption, and the balance between end-user security and the needs of law enforcement are weighty ones and their ultimate resolution will likely take place in Congress and the state legislatures.[5] This Court, however, faces a different set of issues and should not be led astray by Apple's grandstanding.

---

[3] *See* Forgotten Password and Other Sign-in Problems, *http://windows.microsoft.com/en-us/windows-live/account-reset-password-forgot-faq and* Change or Reset the Password of an OS X User Account, https://support.apple.com/en-us/HT202860.

[4] *See* If You Forget the Passcode For Your iPhone, iPad, or iPod Touch, or Your Device is Disabled, *https://support.apple.com/en-us/HT204306* (requiring users to erase their device if they lose the PIN passcode).

[5] Apple participates in the legislative process, spending approximately $12,000,000 on lobbying efforts in the last three years. https://www.opensecrets.org/lobby/clientsum.php?id=D000021754&year=2015, https://www.opensecrets.org/lobby/clientsum.php?id=D000021754&year=2014, https://www.opensecrets.org/lobby/clientsum.php?id=D000021754&year=2013. Apple's lobbying expenditures nearly doubled in 2013, the year that Edward Snowden leaked information regarding the NSA programs, and have since risen every year. *See* Barton Gellman, Aaron Blake, and Greg Miller, *Edward Snowden Comes Forward As Source of NSA Leaks*, WASH. POST (June 9, 2013),

A. *The United States Is Not Requesting Decryption of Personal Data*

Certain politicians, commentators, and law enforcement representatives have advocated for the installation of a chip that would encrypt communications, but contain a "master" key that allows the government to decode encrypted messages. That debate has been proceeding, in one form or another, for over two decades.[6] Lawmakers in New York and California have introduced bills seeking to bar sales of smartphones in those states unless the smartphones provide an avenue for law enforcement to decrypt them.[7] Two congressmen have also recently introduced the ENCRYPT Act, a bill that would preempt such state and local government bans as those being proposed in New York and California.[8] And yet another group of lawmakers has proposed a national commission to determine whether consensus can be reached on any of these issues.[9]

Amici need take no position on these policy disputes, however, because they are not broadly implicated here. This is not an issue of decrypting data. The United States has asked for the limited relief of bypassing two features of Apple's

---

https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

[6] *See, e.g.*, Steven Levy, *Battle of the Clipper Chip*, N.Y TIMES (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.

[7] Assm. Bill No. A8093 (N.Y.): Assm. Bill No. 1681 (Cal.).

[8] H.R. 4528, 114th Cong. (2016) (sponsored by Rep. Ted Lieu (D-CA) and referred to as the ENCRYPT Act of 2016).

[9] Russell Brandom, *New Bill Proposes National Commission on Digital Security*, THE VERGE (Mar. 1, 2016),http://www.theverge.com/2016/3/1/11139838/apple-fbi-congress-national-commission-on-digital-security. Apple has argued that legislative inaction means that All-Writs Act authority cannot exist here, but that is not the case. The All Writs Act is a "residual source of authority to issue writs that are *not* otherwise covered by statute." *Penn. Bureau of Corr. v. United States Marshals Serv.*, 474 U.S. 34, 43 (1985) (emphasis added). Legislative inaction says little about the scope of the All Writs Act. *See Fed. Trade Comm'n v. Dean Foods Co.*, 384 U.S. 597, 609 (1966) ("We cannot infer from the fact that Congress took no action at all on the request of the Commission to grant it or a district court power to enjoin a merger that Congress thereby expressed an intent to circumscribe traditional judicial remedies."). Congress and the state legislatures can hardly have had the final word in light of this ongoing policy debate.

operating system, features that iPhone users can choose to bypass themselves, in order to obtain data on a single phone.[10] This data will likely be lost or destroyed without Apple's assistance. Apple is in possession of, and familiar with, its own code. The United States' request is the most limited means of retrieving the data; certainly, Apple has not proffered any less intrusive means.

Nothing in the Court's order could possibly be construed to require, or even permit as precedent, a requirement that Apple "decrypt" personal data on iPhones. Similarly, there is, and can be, no provision of this order that will require Apple to change the level of security or privacy inherent to the everyday iPhone purchased by the everyday consumer.

Nor is it possible for the Court to craft an order applying to every single iPhone, or smartphone at large, because there is no single technological standard against which to issue such an order. Apple sells numerous different iPhones, each with different operating systems and thus different levels of encryption and security.[11] Apple's chief competitor in the smartphone operating systems market, Google, currently offers eleven proprietary versions of its Android operating system (which go by colorful names as "Froyo" and "Jelly Bean"), and permits users to develop and distribute modified versions, leading to an infinite number of potential Android operating systems.[12] One analyst has explained that, on this

---

[10] *See* Use a Passcode with Your iPhone, iPad, or iPod Touch, https://support.apple.com/en-us/HT204060; Enable Erase Data Option to Delete Data After 10 Failed Passcode Attempts, iOS HACKER, http://ioshacker.com/how-to/enable-erase-data-option-delete-data-10-failed-passcode-attempts.

[11] *See* Katie Benner and Paul Mozur, *Apple Sees Value in Its Stand to Protect Security*, N.Y. TIMES (Feb. 20, 2016), http://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html (reporting that "privacy and security" are part of Apple's brand); Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J. (Sept. 22, 2014), http://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341?cb=logged0.5127165191980588 ("It's not just a feature—it's also a marketing pitch.").

[12] *See* Mark Bergen, *What if San Bernardino Suspect Had Used An Android Instead of an iPhone?*, RE/CODE (Feb. 21, 2016),

issue, "Android is such a mess that you have to distinguish between the Google devices and the zoo of others."[13] Both as a matter of basic jurisdiction and practical reality, the United States' request for relief is narrowly targeted out of respect for the limits of this Court's power. The Court's order is commensurately tailored and appropriate.

B. The United States Is Not Asking Apple to "Hack" Users

Apple asserts that the United States has asked Apple to "hack" its own users. (Ex. 2.) That is a word fraught with meaning—many meanings, in fact. One definition of the word "hack" is to "gain unauthorized access" to data.[14] But that can't be what Apple means here. The access being sought here is not only reasonable, it is authorized by the warrant and the consent of the iPhone's owner. The United States has a right to the data it seeks. Apple toes a fine line when it equates the United States' efforts to legally search a terrorist's phone with indiscriminate "hacking."

Apple's insistence that the United States' request to unlock Farook's iPhone will require Apple to establish "a new 'hacking' department to service government requests," (Apple Br. at 26), is also disingenuous. Prior to 2014, Apple routinely aided the government in accessing locked iPhones under the All Writs Act.[15] Apple already has a well-staffed department in place to handle law enforcement

---

http://recode.net/2016/02/21/what-if-san-bernardino-suspect-had-used-an-android-instead-of-an-iphone/; Android Open Source Project, http://source.android.com

[13] Bergen, *supra* note 12.

[14] Oxford Dictionaries, "hack," http://www.oxforddictionaries.com/us/definition/american_english/hack.

[15] *See, e.g.*, Meg Wagner, *Apple Unlocked At Least 70 iPhones Before Refusing to Hack Into Terrorist's Device*, N.Y. DAILY NEWS (Feb. 18, 2016), http://www.nydailynews.com/news/national/apple-unlocked-70-iphones-refusal-article-1.2536178; Shane Harris, *Apple Unlocked iPhones for the Feds 70 Times Before*, DAILY BEAST (Feb. 17, 2016), http://www.thedailybeast.com/articles/2016/02/17/apple-unlocked-iphones-for-the-feds-70-times-before.html ("Apple has unlocked phones for authorities at least 70 times since 2008.").

requests; indeed, the head of that department, Lisa Olle, filed a declaration in this case.

Another definition of the word "hack" may be more salient here. That definition of "hack" is a noun describing a "piece of computer code providing a quick or inelegant solution to a particular problem."[16] If Apple is using "hack" in that sense, then it is somewhat closer to the mark. The United States is asking Apple to create software, from existing source code, to prevent the destruction of data existing on the iPhone. The code would disable iOS features that all iPhone users are permitted to disable themselves. The software would be a one-off, modified version of iOS—no more and no less.[17]

Nor is Apple being asked to create "malware," unless revising its own operating software is synonymous with "malware." The definition of malware is "software that is intended to damage a computer [or] mobile device . . . ."[18] Apple's application of this term here turns this set of circumstances on its head. (Apple Br. at 2.) The United States is attempting to execute a legal search for, and seizure of, information relevant to a catastrophic crime. The feature it is trying to bypass, and that Apple routinely lets its users bypass on their own, threatens to destroy evidence of the crime.

C. This Is Not A Warrantless Search For Data

Both in the media and in its brief, Apple conflates the United States' request in this case, which is supported by a federal search warrant and due process of law, with the NSA programs established after September 11, 2001. This serves only to

---

[16] Oxford Dictionaries, "hack," http://www.oxforddictionaries.com/us/definition/american_english/hack.

[17] The government's request is by far the safest means of retrieving the data, as Apple can retain custody of its original source code and all modifications, without interference from third-party developers or engineers. From *amici*'s perspective, the United States has gone out of its way to limit the scope of its request and the precedent that may be set in future cases.

[18] Dictionary.com, "malware," http://dictionary.reference.com/browse/malware.

cloud the real issues in this case. While the NSA's PRISM and other data-collection programs may always color the American public's view of the United States's regard for technological privacy, this case involves both a warrant and consent to search. The United States' request is open, public, compliant with the Fourth Amendment, and validated by a neutral magistrate.

D. The United States Has No Interest In Giving "Hackers and Criminals" Access to Information Through A "Backdoor"

Apple claims that ordering its assistance here will inevitably give hackers and criminals "backdoor" access to any iPhone. But to the extent that the ability to bypass this particular security feature on the iPhone 5c exists, Apple created it in the first place—it is inherent in the phone's design. Apple proposes that the United States' request somehow makes it more likely for "hackers and criminals" to exploit a preexisting situation. No matter what word is used to describe it—a "vulnerability," a "flaw," a "backdoor"—it already exists and the United States' request does not change that fact.[19] Since the alleged "backdoor" already exists, "the flaw will inevitably be discovered by the hacker community, or foreign governments down the road. Hiding the flaw does not necessarily improve the security of their customers[.]"[20] What Apple is "being asked to do with respect to *this* device does not reduce the security of other phones."[21] Indeed, Apple is already working on its next version of iOS, which will make the code Apple writes

---

[19] As one cybersecurity expert put it, "In this matter . . . the backdoor thus already exists in the devices and Apple is being asked to show the government how to get in[.]" B. Clifford Neuman, USC INFO. SCI'S. INST., *Why Apple Should Comply With the FBI: Cybersecurity Expert*, CNBC (Feb. 17, 2016), http://www.cnbc.com/2016/02/17/why-apple-should-comply-cybersecurity-expert.html.

[20] Neuman, *supra* note 19. As another technology analyst associated with the American Civil Liberties Union put it, "[t]his bug report has come in the form of a court order." Matt Apuzzo and Katie Benner, *Apple Is Said to be Working on an iPhone Even It Can't Hack*, N.Y. TIMES (Feb. 24, 2016), http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html.

[21] Neuman, *supra* note 19 (emphasis added).

inapplicable in future iOS versions.[22] Apple's doomsday prediction that the United States threatens to subject iPhone users to the wiles of hackers and criminals is just not true.

Moreover, even as Apple frets about the motives of foreign governments, it routinely modifies its systems to comply with the directives of the Chinese government. While portraying itself here as a defender of "civil liberties, society, and national security" (Apple Br. at 5), Apple has complied with China's censorship laws and moved all Chinese users' iCloud data from Apple's secure cloud to a datacenter located in China that is owned and operated by a state-owned telecom company.[23] Since 2015, Apple also submits its products, including the iPhone, to Chinese government security audits.[24]

Apple benefits immensely from its conciliatory relationship with the Chinese government, selling $59 billion worth of Apple products there just last year, with China now becoming the number one buyer of iPhones in the world.[25] China has also now approved Apple's proprietary Apple Pay system.[26] The United States,

---

[22] *See* Mark Sullivan, *Now Apple Could Make the iPhone 7 Even Harder to Unlock*, FAST COMPANY (Feb. 24, 2016), http://www.fastcompany.com/3057121/now-apple-could-make-the-iphone-7-even-harder-to-unlock.

[23] *See* Sam Oliver, *Apple Agrees to Subject Products to Chinese Government Security Audits – Report*, APPLEINSIDER (JAN. 22, 2015), http://appleinsider.com/articles/15/01/22/apple-agrees-to-subject-products-to-chinese-government-security-audits---report; Margi Murphy, *Apple News Blocking is a Reminder of the Ethical Minefield Facing Tech Firms in the Chinese Market*, TECHWORLD (Oct. 13, 2015), http://www.techworld.com/social-media/chinas-blocking-blitz-should-companies-be-complicit-in-chinese-censorship-3627221.

[24] Oliver, *supra* note 23; Joon Ian Wong, *Apple is Openly Defying U.S. Security Orders, But In China It Takes a Very Different Approach*, QUARTZ (Feb. 17, 2016), http://qz.com/618371/apple-is-openly-defying-us-security-orders-but-in-china-it-takes-a-very-different-approach/.

[25] David Pierson, *While It Defies U.S. Government, Apple Abides By China's Orders—And Reaps Big Rewards*, L.A. TIMES (Feb. 26, 2016), http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html.

[26] *Id.*

meanwhile, has no golden carrot to offer Apple to ensure compliance with its laws as growth in sales of Apple's products in the United States has stagnated.[27]

E. Apple's Slippery-Slope Arguments Are Speculative

Because the Court's order does not fit neatly into the usual boxes, the best Apple can do is resort to a "slippery slope" argument: Requiring Apple under these circumstances to bypass security features it built into this iPhone, *ipso facto*, defeats security on all iPhones. *Amici* cannot conceive how this could be the case. No court could possibly arrogate to itself the power to set nationwide, even global, encryption standards on smartphone technology. The Court's jurisdiction here is appropriately limited, and its order appropriately modest. The United States legally possesses the phone. Apple has the means to assist the United States' search, as it maintains significant control over the iPhone's operating software, and has the technological acumen and resources to do so.[28] Meanwhile, the only party with any conceivable privacy interest in this phone, the County, wants the phone to be searched, and the United States has agreed to allow Apple to retain custody over any fix that will bypass the self-destruct mechanism.

Because the Court's order is so limited, Apple's primary concern on this score appears to be the precedential value of the Court's order. It fears that if required to create the code necessary to bypass this iPhone's security, it will either be the case that (1) other courts will use the Court's order as precedent to order more burdensome and dangerous action in future cases, or (2) Congress or state legislatures will be emboldened to move forward with policies that Apple believes are destructive to its business model.

---

[27] *Id.*

[28] The terms of use on iOS make clear that it is licensed from Apple. Apple "retain[s] ownership of the iOS Software itself and reserve[s] all rights not expressly granted" to the consumer. *See* Software License Agreements, iPad, iPhone, and iPod Touch Terms and Conditions, http://www.apple.com/legal/sla/.

As to the former, this case certainly presents the conditions—a mass murder by terrorists implicating national-security interests—where requiring Apple's technical assistance is at its apex, given the overriding and obvious public interest in completing the United States' investigation. The All Writs Act is well-suited to individualized determinations of the facts of any particular request for assistance. And on the particular and specific facts of *this* case, compelling Apple's assistance with execution of the United States' valid search warrant is justified.[29] As to the latter, whether legislators ever devise a law requiring greater cooperation from technology companies with law enforcement is irrelevant to this Court's legal analysis today.

III. The All Writs Act Analysis Takes Into Account The Extraordinary Circumstances Underlying The United States' Request

Apple has focused on the unique and unprecedented nature of the United States' request as reason to oppose the order. As an initial matter, Apple's observation that the request is unprecedented proves very little. The plain fact is that technology evolves, and the scope of the All Writs Act naturally changes with it. Less than two years ago, Apple routinely complied with search warrants and All Writs Act requests from law enforcement, even on locked iPhones, and thus there was no need for an All Writs Act request like this one.[30] Apple has now

---

[29] Already, Apple's argument on this issue is weakened by the order issued just a few days ago by Magistrate Judge James Orenstein in another All Writs Act case in the Eastern District of New York. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By This Court*, Case No. 1:15-mc-01902-JO, Dkt. No. 29 (E.D.N.Y. Feb. 29, 2016). Indeed, Magistrate Judge Orenstein left open the potential for a case, or cases, where "the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate society interests arrayed against it here." (*Id.* at 48.) *Amici* respectfully suggest this is such a case.

[30] *See* Andy Greenberg, *Despite Apple's Privacy Pledge, Cops Can Still Pull Data Off a Locked iPhone*, WIRED (Sept. 18, 2014), http://www.wired.com/2014/09/apple-iphone-security.

attempted to evolve its iPhone operating system so that it falls outside the ambit of CALEA and, thus, does not have to comply with valid legal process from state and local governments.[31] However, no citizen of the United States, corporate or otherwise, should be able to claim that the law does not apply to them; Apple cannot innovate itself out of the All Writs Act. The All Writs Act extends "under appropriate circumstances" to those who are "in a position to frustrate the implementation of a court order or the proper administration of justice." *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Apple is in such a position and the Court's entry of an order compelling Apple to comply with the search warrant is proper in these specific and limited circumstances.

Indeed, the Supreme Court has recognized that the All Writs Act can justify extraordinary action in special circumstances. For example, in *Pennsylvania Bureau of Correction*, the Supreme Court held that the United States Marshals Service could not be compelled by the All Writs Act to transport a state prisoner to the federal courthouse, but stated that an All Writs Act order directing federal marshals to transport a state prisoner may be appropriate in "exceptional circumstances . . . such as where there are serious security risks." 474 U.S. 41, 43 (1985); *see also In re Application of United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone* [*In re Application*], 849 F. Supp. 2d 526, 582 (D. Md. 2011) ("[T]he All Writs Act may authorize a search in furtherance of a prior order only where no other law applies no Fourth Amendment right to privacy is implicated, and exceptional circumstances are present.").[32] The extraordinary circumstances of this case—the

---

[31] To suggest that Congress has had the final word on technology that has only just come into being, and which is by its nature ever-evolving, is presumptive to say the least.

[32] The Maryland case contrasts well with this case, and demonstrates the inherent protections in All Writs Act analysis. In that case, the government's request was rejected because the government was attempting to "circumvent the requirements of the Fourth Amendment." *In re Application*, 849 F. Supp. 2d at 582. There is no Fourth Amendment concern here. *See supra* Part I.

monumental interest in investigating this particular crime, weighed against the complete lack of Fourth Amendment concern and Apple's unique ability to assist as requested—warrants relief here.

IV. Apple's Constitutional Arguments Are Unsupported by Both Case Law and the Facts

Apple makes two constitutional arguments in support of its Motion to Vacate. First, Apple argues that the Court's order directing Apple to comply with a valid search warrant somehow violates the Fourteenth Amendment's[33] guarantee of substantive due process. (Apple Br. at 34.) Second, Apple argues that the Court's order compels speech in violation of the First Amendment. (*Id.* at 32.) Neither argument carries water.[34]

A. Apple's Substantive Due Process Claim Should Be Dismissed as it is an Improperly Pled Fourth Amendment Claim and Because the Court's Order is not Clearly Arbitrary or Unreasonable

Substantive due process "protects individuals from arbitrary deprivation of their liberty by government." *Costanich*, 627 F.3d at 1110 (quoting *Brittain v. Hansen*, 451 F.3d 982, 991 (9th Cir. 2006)). However, where another constitutional amendment "provides an explicit textual source of constitutional protection" against a particular sort of government behavior," a court must assess the claims under that explicit provision and "not the more generalized notion of substantive due process." *Conn v. Gabbert*, 526 U.S. 286, 293 (1999) (quoting

---

[33] Apple's brief cites to the Fifth Amendment, but the cases that Apple cites interpret the Fourteenth Amendment's guarantee of substantive due process, not the Fifth's. *See, e.g.*, *County of Sacramento v. Lewis*, 523 U.S. 833, 836 (1998); *Costanich v. Dep't of Social and Health Servs.*, 627 F.3d 1101, 1107-08 (9th Cir. 2010).

[34] Apple also unconvincingly argues that this issue presents a non-justiciable political question. (Apple Br. at 19.) That argument can be dismissed out of hand. The validity of a search warrant and the Court's power to enforce compliance with a search warrant has always been a legal question. *See, e.g.*, *United States v. New York Tel. Co.*, 434 U.S. 159 (1977), *In the Matter of the Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities*, 616 F.2d 1122 (9th Cir. 1980).

Graham v. Connor, 490 U.S. 386, 395 (1989)). In this case, Apple's Fourteenth Amendment argument is essentially that the search warrant is not "reasonable" because its enforcement requires Apple's assistance—assistance Apple declines to give. Whether a search and seizure is "reasonable" is explicitly addressed under the Fourth Amendment, not with a substantive due process claim. This claim should therefore be dismissed.

But even if the Court chooses to entertain this claim, Apple cannot prevail. To establish a substantive due process claim, Apple must show "a government deprivation of life, liberty, or property." *Costanich*, 627 F.3d at 1110 (quoting *Nunez v. City of Los Angeles*, 147 F.3d 867, 871 (9th Cir. 1998)). Apple must also show that such deprivation was "clearly arbitrary and unreasonable, having no substantial relation to the public health, safety, morals, or general welfare." *Sinaloa Lake Owners Ass'n v. City of Simi Valley*, 864 F.2d 1475, 1484 (9th Cir. 1989) (quoting *Village of Euclid v. Ambler Realty Co.*, 272 U.S. 365, 395 (1926)). A court order requiring Apple to assist law enforcement with accessing the iPhone of a terrorist in a matter of national security pursuant to a legally valid search warrant has a substantial relationship to public safety and the general welfare, and is neither arbitrary nor unreasonable. Apple may not like the court order, but Apple's distaste for cooperation with law enforcement does not rise to the level of a constitutional violation.

B. The Court's Order Does Not Violate Apple's First Amendment Rights Because it Lawfully Compels Commercial Speech in the Form of Functional Code

Apple's First Amendment argument is that (a) some courts have held that computer code is speech under the First Amendment; and (b) the United States is compelling Apple's assistance to write computer code, *ergo*, the government is compelling speech and must satisfy a strict-scrutiny standard. (Apple Br. at 32-

33.) But the true nature of the "speech" compelled here is that of commercial, functional code. It does not merit full First Amendment protection.

Some courts have held that computer code is subject to First Amendment protection. *See, e.g.*, *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449-50 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 482 (6th Cir. 2000); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002). But those cases involve computer code with an expressive or informative nature (a "speech component") and a functional nature (a "nonspeech" component). *See Corley*, 273 F.3d at 451, 454; *Junger*, 209 F.3d at 484; *see also Elcom*, 203 F. Supp. 2d at 1128-29 (stating that courts must divorce "the function from the message"). Only the expressive or informative nature of code is subject to the full panoply of First Amendment rights; solely functional code "is not speech within the meaning of the First Amendment." *Corley*, 273 F.3d at 454; *see also id.* at 452 ("The functionality of computer code properly affects the scope of its First Amendment protection."); *Commodity Futures Trading Comm'n v. Vartuli*, 228 F.3d 94, 111 (2d Cir. 2000) (holding that software that is automatic and is to be "used in an entirely mechanical way" is not speech under the First Amendment); *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 386 (1969) ("[D]ifferences in the characteristics of new media justify differences in the First Amendment standards applied to them."). Because functional code is not speech, it can be regulated so long as the regulation services "a substantial government interest," the interest is "unrelated to the suppression of free expression," and any incidental restriction on speech "must not burden substantially more speech than is necessary to further that interest." *Corley*, 273 F.3d at 454; *see also Junger*, 209 F.3d at 485 (stating that computer code should be analyzed under the intermediate scrutiny test); *Elcom*, 203 F. Supp. 2d at 1129 (applying intermediate scrutiny).

The code that the United States seeks to obtain is functional code—it accomplishes nothing more than unlocking a single iPhone so that the information

located on it can be properly seized pursuant to the search warrant. This is the electronic equivalent of unlocking a door—no expression is involved at all.

Further, the United States' request is "unrelated to the suppression of free expression." *Corley*, 273 F.3d at 454. The United States' interest here is investigating a terrorist act. National security interests "can outweigh the interests of protected speech and require the regulation of speech." *See Junger*, 209 F.3d at 485. Nor does the United States' request "burden substantially more speech than is necessary to further" its interest in investigating terrorism. *Corley*, 273 F.3d at 454. The United States has asked for code to bypass the PIN passcode functionality of a single iPhone, a bypass that will be obsolete by the next iOS software update. Moreover, the United States has not asked Apple to change a single expressive or informative aspect of the iOS. The United States' request, and the Court's order, satisfies intermediate scrutiny and thus the First Amendment provides Apple no solace in resisting the search warrant.

Apple attempts to evade the intermediate scrutiny test by arguing that the Court's order violates the First Amendment by compelling Apple to unwillingly write code. According to Apple, compelled speech is subject to the strict scrutiny test. (Apple Br. at 32.) Apple, however, is not a private citizen and it is not being asked to engage in political oratory—it is a corporation asked to write commercial code for a commercial product, in a single instance fraught with national-security implications. Apple's decisions to program in closed-source code, to encrypt its iPhones, and to design the PIN passcode lock are all commercial decisions to increase iPhone sales.[35] This case is therefore, at best, about compelled

---

[35] *See* Sam Thielman, *Apple's Encryption Battle with the FBI Has Implications Well Past the iPhone*, THE GUARDIAN (Feb. 20, 2016), http://www.theguardian.com/technology/2016/feb/19/apple-fbi-privacy-encryption-fight-san-bernardino-shooting-syed-farook-iphone (stating that Apple's "biggest selling point these days is privacy" and "the quest to build devices that can be sold on the promise of greater security is a point of differentiation between Apple and its competitors"); Peter Bergen, *Billions at Stake in Apple Encryption Case*, CNN (Feb. 20, 2016), http://www.cnn.com/2016/02/19/opinions/apple-vs-

commercial speech, not core, private First Amendment speech. *See Zauderer v. Off. of Disciplinary Counsel of Supreme Ct. of Ohio*, 471 U.S. 626, 651 (1985) (stating that there is a distinct difference in First Amendment protection between the government prescribing speech regarding commerce and the government prescribing "what shall be orthodox in politics, nationalism, religion, or other matters of opinion") (citation omitted).

The Constitution "accords a lesser protection to commercial speech than to other constitutionally guaranteed expression." *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 562-63 (1980). The protection available for a "particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation." *Id.* at 563. Compelled commercial speech is subject either to the intermediate scrutiny test of *Central Hudson* or the rational basis test of *Zauderer*. *See Nat'l Mfrs. Ass'n v. Sorrell*, 272 F.3d 104, 114-15 (2d Cir. 2001) (holding that "mandating that commercial actors disclose commercial information" is subject to the rational basis test); *A Woman's Friend Pregnancy Clinic v. Harris*, No. 2:15-cv-02122-KJM-AC, 2015 WL 9274116, at *15 (E.D. Cal. Dec. 21, 2015) (*quoting Zauderer*, 471 U.S. at 651); *see CTIA-The Wireless Ass'n v. City of Berkeley*, --- F. Supp. 3d ---, 2015 WL 5569072, at *12 (N.D. Cal. Sept. 21, 2015) (stating that *Zauderer* "suggests that compelled disclosure of commercial speech . . . is subject to rational basis review rather than intermediate scrutiny"). Under either level of review, the Court's order does not unconstitutionally impede Apple's First Amendment rights.[36]

---

fbi-on-encryption-bergen (noting that Apple's concern is losing "tens of billions of dollars and . . . market share"); *see also* Apple Br. at 5 (noting "Apple's Industry-Leading Device Security").

[36] The Northern District of California has held that where compelled commercial speech is clearly identified as government speech, a standard "even less exacting than [rational basis] should apply." *See CTIA*, --- F. Supp. 3d ---, 2015 WL 5569072, at *14 (N.D. Cal. Sept. 21, 2015). The speech being requested here is compelled government speech, a point Apple itself notes by referring to the code as "GovtOS." *See id.* at *15 (stating that where there is "attribution of the compelled speech to someone other than the speaker"—in particular, the

Analyzing compelled commercial speech through *Central Hudson's* intermediate scrutiny test involves weighing three factors: (1) whether the government asserts "a substantial interest to be achieved" by the compelled speech; (2) the compelled speech is "in proportion to that interest[;]" and (3) the compelled speech is "designed carefully to achieve" the government's interest, that is, that the compelled speech directly advances the governmental interest involved and the interest could not be served as well by a more limited compulsion. *Cent. Hudson*, 447 U.S. at 564. Under *Zauderer*'s rational basis test, compelled commercial speech is constitutional so long as the compulsion is reasonably related to a legitimate government interest. *See Zauderer*, 471 U.S. at 651; *Am. Meat Inst. v. United States Dept. of Agric.*, 760 F.3d 18, 23 (D.C. Cir. 2014); *N.Y. State Restaurant Ass'n v. New York City Bd. of Health*, 556 F.3d 114, 134 (2d Cir. 2009).

The United States has a legitimate and extensive interest in investigating this terrorist act, an investigation that could provide closure to surviving victims and loved ones left behind. The Court's order compelling Apple to bypass the PIN passcode on a single iPhone utilized by one of the terrorists is reasonably related to that interest. *Zauderer*'s rational basis test is thus satisfied. Furthermore, the Court's order is proportional to the government's interest and carefully designed to achieve that interest. The Court's order is limited to the single iPhone, and only for the purpose of retrieving the necessary data relevant to the investigation. Certainly, Apple has identified no less intrusive manner to recover the iPhone data the United States is entitled to recover under the warrant. *Central Hudson*'s test is therefore satisfied as well. Whatever Apple's limited First Amendment interests are, they are not violated by the Court's order.

---

government—the *Zauderer* factual-and-uncontroversial requirement is not needed to minimize the intrusion upon the plaintiff's First Amendment interest). Thus, from the perspective of Apple's First Amendment rights, it can be compelled to create this code on a showing of even less than a rational basis.

CONCLUSION

This case is not what Apple is making it out to be. To obtain sympathy for its cause, Apple would like to portray this case as one in which the privacy interests of millions of Americans are at stake. As *amici* have demonstrated, no such privacy interests are implicated here. What is implicated here is the United States' ability to obtain and execute a valid warrant to search one phone used by a terrorist who committed mass atrocities. If there is any situation that warrants extraordinary relief under the All Writs Act, *amici* submit that it is, in fact, this one. The Court's order requiring Apple's assistance to retrieve the data on Farook's iPhone should stand.

Dated: March 3, 2016

LARSON O'BRIEN LLP

By: 

Stephen G. Larson
Attorneys for *Amicus Curiae*
Greg Clayborn, James Godoy, Hal Houser, Tina Meins, Mark Sandefur, and Robert Velasco

EXHIBIT 1

Dear Mr. Cook,

Our son, Larry Daniel Eugene Kaufman, was one of the fourteen people killed in the terrorist shooting in San Bernardino. Daniel worked as an instructor, teaching people with disabilities the skills necessary to live independent lives. He was not what one would think of as a terrorist target of the Islamic State.

I know that you are facing some difficult decisions concerning letting the FBI develop a program to break into the iPhone that one of the murderers had with them. I'd like to ask you to support the requests from the FBI.

My reasons are from a different perspective. I have attended private briefings that are held for the families of the victims. At these briefings, we learn first-hand what the public eventually learns. We are not privy to anything *only* the FBI knows, but we talk amongst ourselves about the horrors of that day. Some of the survivors come to these meetings pushing walkers, or limping with canes. They are reminders to me of what they went through. We who lost our family members are reminders to them that it could have been worse. Several of the survivors tell me bone-chilling stories of where they were, and what they saw. Some of them describe in precise detail, laying on the floor, hiding under furniture and the bodies of their co-workers, that they saw *three* assailants, not two, walking around in heavy boots as they carried out their murders.

I have seen demonstrations of the tricks one's mind plays in times of terror. Witnesses swear they saw different things. Time stretches. People misidentify perpetrators. And this may be what happened. Perhaps they were wrong about seeing three terrorists.

But, consider that there are several witnesses who saw three killers. Consider that the FBI did not recover any "heavy boots" in their thorough searches. If you talked with these witnesses, as I have, you too would be convinced that there were three.

Recovery of information from the iPhone in question may not lead to anything new. But, what if there is evidence pointing to a third shooter? What if it leads to an unknown terrorist cell? What if others are attacked, and you and I did nothing to prevent it?

Please also consider that the software you have been asked to write undoubtedly already exists in the security services of Communist China, and many other countries, who have already reverse-engineered the iPhone operating system for future exploitation. Why should we be the ones without it?

I urge you to consider the requested cooperation as your patriotic duty.

With the greatest respect,

Mark M. Sandefur

EXHIBIT 2

February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

Answers to your questions about privacy and security ›

The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.

The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point,

we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.

We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.

Tim Cook

Answers to your questions about privacy and security >

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

Case No: 5:16-CM-00010 (SP)

PROOF OF SERVICE

I am a citizen of the United States. My business address is Larson O'Brien LLP, 555 S. Flower Street, Suite 4400, Los Angeles, CA 90071. I am employed in the County of Los Angeles where this service occurs. I am over the age of 18 years, and not a party to the within cause.

On the date set forth below, according to ordinary business practice, I served the foregoing document(s) described as:

APPLICATION OF GREG CLAYBORN, JAMES GODOY, HAL HOUSER, TINA MEINS, MARK SANDEFUR, AND ROBERT VELASCO TO FILE AN *AMICUS CURIAE* BRIEF

☐ (BY CM/ECF) I hereby certify that on this date, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants (if any) indicated on the Manual Notice list.

☐ (BY FAX) I transmitted via facsimile, from facsimile number 213-623-2000, the document(s) to the person(s) on the attached service list at the fax number(s) set forth therein, on this date before 5:00 p.m. A statement that this transmission was reported as complete and properly issued by the sending fax machine without error is attached to this Proof of Service.

☐ (BY E-MAIL) On this date, I personally transmitted the foregoing document(s) via electronic mail to the e-mail address(es) of the person(s) on the attached service list.

☐ (BY MAIL) I am readily familiar with my employer's business practice for collection and processing of correspondence for mailing with the U.S. Postal Service, and that practice is that correspondence is deposited with the U.S. Postal Service the same day as the day of collection in the ordinary course of business. On this date, I placed the document(s) in envelopes addressed to the person(s) on the attached service list and sealed and placed the envelopes for collection and mailing following ordinary business practices.

☐ (BY PERSONAL SERVICE) On this date, I delivered by hand envelope(s) containing the document(s) to the persons(s) on the attached service list.

☒ (BY OVERNIGHT DELIVERY) On this date, I placed the documents in envelope(s) addressed to the person(s) on the attached service list, and caused those envelopes to be delivered to an overnight delivery carrier, with delivery fees provided for, for next-business-day delivery to whom it is to be served.

☒ (Federal) I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on March 3, 2016 at Los Angeles, California.

Yvonne Gutierrez

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

Case No: 5:16-CM-00010 (SP)

SERVICE LIST

Allen W. Chiu AUSA – Office of US Attorney National Security Section 312 North Spring Street, Ste 1300 Los Angeles, CA 90012 Tel: 213.894.2435 Fax: 213.894-6436 Email: allen.chiu@usdoj.gov	Attorneys for Plaintiff, USA
Tracy L. Wilkison AUSA Office of US Attorney Chief, Cyber and Intellectual Property Crimes Section 312 North Spring Street, 11th Floor Los Angeles, CA 90012-4700 Tel: 213.894-0622 Fax: 213.894.0141 Email: tracy.wilkison@usdoj.gov	Attorneys for Plaintiff, USA
Theodore J. Boutrous, Jr. Gibson Dunn and Crutcher LLP 333 South Grand Avenue Los Angeles, CA 90071-3197 Tel: 213. 299. 7000 Fax: 213. 229.7520 Email: tboutrous@gibsondunn.com	Attorneys for Respondent, *Apple Inc.*