ARTICLES

WILLAMETTE LAW REVIEW

52:4 Summer 2016

MAKING APPLESAUCE: REFLECTIONS ON APPLE'S IPHONE CASE

HONORABLE PAUL J. DE MUNIZ*
DISTINGUISHED JURIST IN RESIDENCE, WILLAMETTE UNIVERSITY COLLEGE OF LAW

PRIVACY LAW SYMPOSIUM KICK-OFF ADDRESS | FEBRUARY 26, 2016

Editor's Note: *This address was given to the attendees of Willamette Law Review's Annual Symposium on February 26, 2016, focusing on Privacy and Data Security Law. It is preserved in its original form. Although the issue of the FBI unlocking the iPhone has since been resolved*[1] *without making its way through the legal system, the issues discussed in this speech are ongoing concerns in the privacy law field.*

**Retired Chief Justice of the Oregon Supreme Court*

[1] Ellen Nakashima, *FBI Paid Professional Hackers One-time Fee to Crack San Bernardino iPhone*, THE WASHINGTON POST, Apr. 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html ("The FBI cracked a San Bernardino terrorist's phone with the help of professional hackers who discovered and brought to the bureau at least one previously unknown software flaw . . . ."); Mark Hosenball, *FBI Paid Under $1 Million to Unlock San Bernardino iPhone: Sources*, REUTERS, May 4, 2016, http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032 ("The Justice Department unlocked [Farook's iPhone] in March with the help of [an undisclosed] contractor after Apple Inc refused to bypass the device's encryption features on grounds it could undermine security for all users.").

I. INTRODUCTION

Good morning. Thank you, Curtis, for that very kind introduction. It is a pleasure to be a small part of this very interesting Symposium. Like you, I am very interested in what our expert speakers have to tell us today. And thanks to all of you for taking time from your busy schedules to attend today's Symposium. However, before we get to the meat and potatoes, so to speak, from our privacy law experts today, I have been given the privilege of making some brief remarks about the big, hulking elephant in the room—the San Bernardino Apple iPhone case that's in the news. Unless you've been living under a rock, or for students here who have not looked up from a casebook in months, you've heard of Apple's recent fight with the FBI. I'll begin by taking a snapshot of where the parties stand and what the key issues are for both sides. I will conclude by attempting to identify key legal issues that may arise as the case progresses.

Yesterday, I read in the *New York Times* that Apple had hired the Teds—Ted Olson and Ted Boutrous of Gibson Dunn firm—both great lawyers. You may recall that although Ted Olson was Solicitor General for a time in the Bush Administration, he teamed up a few years ago with David Bois, his opponent in *Bush v. Gore*, to win *Hollingsworth v. Perry*, the Gay Marriage case from California.[2] Ted Olson also argued and won the *Massey Coal* case,[3] in which the Supreme Court reversed the West Virginia Supreme Court decision in favor of Massey Coal after Justice Brent Benjamin of the West Virginia Supreme Court refused to recuse himself from the case, even though Don Blankenship, the owner of Massey Coal, had given Justice Benjamin $3 million in support of his election to the West Virginia Supreme Court. Ted served on the board of the National Center for State Courts and I got to meet him when I served on the board of the Conference of Chief Justices. And, Ted Boutrous is no

[2] Hollingsworth v. Perry, 133 S. Ct. 2652 (2013) (holding petitioners, who challenged California's ballot initiative Proposition 8 banning same-sex marriage, did not have Article III standing to appeal in federal court after California refused appeal).

[3] Caperton v. A.T. Massey Coal Co., Inc., 556 U.S. 868 (2009) (holding that Due Process requires a judge to recuse himself when the "probability of actual bias on the part of the judge or decision-maker is too high to be constitutionally tolerable.").

stranger to Oregon. He argued in the Oregon Supreme Court in 2010 on behalf of Farmers Insurance in the very important *Strawn v. Farmers*[4] case. He did not prevail in that case, although he did get one vote in a dissent written by current Chief Justice Thomas Balmer. As talented and experienced as they are, I think the Teds will have their work cut out for them in the iPhone case. Their reply brief on behalf of Apple is due today.

II. BACKGROUND

A. San Bernardino Terrorist Attack

The iPhone case arises from the San Bernardino massacre in 2015 at the Inland Regional Center. You will recall that on December 2, 2015, Syed Rizwan Farook and his wife, Tafsheen Malik, stormed the Inland Regional Center and opened fire, killing fourteen people and injuring twenty-two more. Farook and Malik were killed following the attack.[5]

B. Federal Search Warrant Issued for Black Lexus

The day after the attack, a U.S. Magistrate Judge, issued a search warrant for the search of a black Lexus that was believed to be connected to the suspects.[6] The iPhone in question was found in the car.[7]

Farook didn't own the iPhone. The iPhone was owned by Farook's employer, the San Bernardino County Department of Public Health, which immediately consented to the government's search of the phone.[8] Right away, that knocked out any Fourth Amendment claim that a search of the phone would be an unreasonable search and seizure. Interestingly (or ironically), the public health department was at that very time testing out a trial software that employers perhaps

[4] Strawn v. Farmers Ins. Co. of Oregon, 297 P.3d 439 (2013).

[5] Erik Ortiz, *San Bernardino Shooting: Timeline of How the Rampage Unfolded*, NBC NEWS, Dec. 3, 2015, http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bern ardino -shooting-timeline-how-rampage-unfolded-n473501.

[6] In re Search of Black Lexus 1S300 California License Plate #5kgd203, handicap placard 360466F, Vehicle Identification No. JTHBD192X50094434, No. ED 15-0451M (C.D. Cal. Dec. 3, 2015) (order granting search and seizure).

[7] Andrew Blankstein, *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone*, NBC NEWS, Feb. 16, 2016, http://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701.

[8] *Id.*

could use to breach its employer-owned locked electronic devices.

However, it was the policy of the public health department at that time to issue iPhones to its employees equipped with the auto-erase, ten-wrong-passwords-and-you're-done feature.[9] Farook had set his own password, and knowledge of the password died with Farook.

The government alleges in its brief that the FBI is unable to search the phone because the auto-erase function would erase the phone's contents if ten erroneous passcodes are entered.[10] Since it is impossible to tell from the locked screen whether the auto-erase function is enabled, the FBI is not actually sure whether Farook's phone has the auto-erase function enabled. Hence, the FBI simply can't repeatedly try to guess the passcode on Farook's phone.

Obviously, Apple made the iPhone, coded it, and has the ability to circumvent the passcode lock. Interestingly enough, Apple has done this for older iPhones in similar situations that ran on older operating systems.

C. The Court's Order

The federal court order requires Apple to provide "reasonable technical assistance" to the government and to do three things:

(1) Bypass or disable the auto-erase function;

(2) Allow the FBI to "submit," not "enter," passcodes to the device; and

(3) Ensure that the device's software doesn't create any additional delay when the FBI submits passcodes.[11]

Apple can also comply with the court's order if it plays ball in another way that is agreeable with the government. Of course, Apple can challenge the order if it can show that "[complying] with [the] order would be unreasonably burdensome."[12]

At this point we might ask a very basic question: How did Apple—not a party to any matter involving the San Bernardino

[9] In the Matter of Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, slip op. at 2, 6 (C.D. Cal. Feb. 16, 2016).

[10] *Apple vs. FBI: Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone*, ELECTRONIC PRIVACY INFO. CENTER (July 24, 2016), https://epic.org/amicus/crypto/apple/#legal.

[11] In the Matter of Search of an Apple iPhone, *supra* note 9 (order compelling Apple Inc. to assist agents in search).

[12] *Id.*

massacre—become subject to a federal court order? To answer that question, we've got to go back past the iPhone, Apple, and Steve Jobs; we've got to go back 227 years to the All Writs Act of 1789.

III. OLD LAW WITH A NEW APP(LICATION)

The All Writs Act of 1789 is refreshingly brief but broad, providing that:

> (a) The Supreme Court and all courts established by Act of Congress *may issue all writs necessary* or appropriate in aid of their respective jurisdictions and agreeable to the *usages and principles of law*.
>
> (b) An alternative writ or *rule nisi* may be issued by a justice or judge of a court which has jurisdiction.[13]

The text of the act is instructive, using terms like *necessary*, *appropriate*, *usages*, and *principles*. But what is *necessary*? What is *appropriate*? What *principles*?

In its brief, the government cites a Ninth Circuit opinion, *Plum Creek Lumber Co. v. Hutton*,[14] in support of its argument that a court, with the aid of a valid warrant, has the power under the All Writs Act to "order a third party to provide nonburdensome technical assistance to law enforcement officers."[15]

The Supreme Court has previously explained the All Writs Act. In *United States v. New York Telephone Co.*, the FBI wanted to surveil an illegal gambling enterprise in New York City.[16] The FBI establishsed probable cause, and the district court directed the telephone company to help the FBI install number-recording devices on the telephone company's lines.[17] The court's order required the New York Telephone Company to give the FBI "all information, facilities, and technical assistance" to intercept the crooks' calls.[18]

[13] 28 U.S.C. § 1651 (2016) (emphasis added).

[14] Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283 (9th Cir 1979).

[15] In re Search of an Apple iPhone, Gov't *ex parte* Application for Order Compelling Apple Inc. to Assist Agents in Search (C.D. Cal. Feb. 16, 2016) (No. CM-16-10); 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 (C.D. Cal. Feb. 16, 2016) (No. ED 15-0451M) (citing Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979)).

[16] United States v. New York Tel. Co., 434 U.S. 159, 162 (1977).

[17] *Id.* at 163.

[18] *Id.* at 176.

The telephone company moved to vacate the court's order, but the court answered that it had authority to issue the order under the All Writs Act.[19]

The Supreme Court agreed with the district court.[20] The Supreme Court observed that the All Writs Act permits a court to use its judgment to "achieve the rational ends of the law."[21] The Court held in that case that:

> the power conferred by the [All Writs] Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.[22]

So, the Act's power extends to "persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice."[23]

Now, two things are clear: (1) the All Writs Act encompasses those who haven't taken any affirmative action yet, and (2) the Act applies to nonparties. Here, that means Apple.

IV. RESIDUAL AUTHORITY

The All Writs Act is a residual source of authority for courts. For example, the Supreme Court explained that under the Act courts can issue orders that are not covered by a regular statute.[24]

In *Pennsylvania Bureau of Correction v. U.S. Marshals Service*, an inmate sued state prison officials under 42 U.S.C. § 1983.[25] The district court transferred the case to a federal magistrate judge, and the magistrate issued writs of habeas corpus *ad testificandum*[26] to produce

[19] *Id.* at 163.

[20] *Id.* at 172.

[21] *Id.* (citing Harris v. Nelson, 394 U.S. 286 (1969)).

[22] *Id.* at 174 (internal quotations omitted).

[23] *Id.*

[24] Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

[25] *Id.*

[26] *ad testificandum,* BALLENTINE'S LAW DICTIONARY (3d ed. 1969) (an order to appear and testify).

five witnesses. Since the witnesses were scattered in different prisons throughout Pennsylvania, the magistrate ordered state prison wardens to transport the inmates to the county jail nearest to the federal courthouse in Philadelphia. The orders also commanded the U.S. Marshals to transport inmates from the county facility to the federal court, guard them during trial, and transport them back to the county facility. The magistrate tried to use the All Writs Act to force the Marshals to transport and guard state inmates who were called to testify in federal litigation, but the Supreme Court reversed the lower court's order.

The Court held that the magistrate used the All Writs Act incorrectly. To get there, the Court worked forward from § 14 of the Judiciary Act of 1789. The Court first considered the original language of the Judiciary Act of 1789. The original language of § 14 allows courts to issue writs of *scire facias*,[27] *habeas corpus*, and "*all other writs* not specifically provided for by statute which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law."[28] The Court explained that its early view of the all-writs provision applied the provision to "filling the interstices of federal judicial power when . . . gaps threatened to thwart the otherwise proper exercise of federal courts' jurisdiction."[29]

In short, the Court always understood the all-writs provision to be a gap filler. Since the Judiciary Act of 1789 codified the *ad testificandum* writ in the same section as the all-writs provision, there was no gap to fill; the all-writs provision can't be used alongside the writ of *ad testificandum*.[30] Interestingly, while Congress cut out the "not specifically provided for by statute" language in 1948, the Court forged ahead with its 18th-century understanding of the provision. The Court kept its interpretive course because it found that legislative history looked favorably on a 1945 Supreme Court decision to prohibit the writ where an alternate statutory scheme existed.[31]

Ultimately, for our purposes, *Pennsylvania Bureau of Correction*

[27] *scire facias*, BLACK'S LAW DICTIONARY (10th ed. 2014) (a writ requiring the person against whom it is issued to appear and show cause why some matter of record should not be enforced, annulled, or vacated, or why a dormant judgment against that person should not be revived).

[28] Pa. Bureau of Corr., supra note 24, at 43.

[29] *Id.*

[30] *Id.*

[31] *See* U.S. Alkali Exp. Ass'n. v. United States, 325 U.S. 196 (1945).

v. U.S. Marshals Service stands for the rule that a court can't use the writ as a backup or a substitute. The Supreme Court explained that "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling."[32] That's important here, in the Apple case, because the government is arguing that there isn't a statute that's directly on point.

V. APPLYING THE ACT

But what about applying the Act? There are three factors that the court used in *New York Telephone* to determine whether the writ can be issued. These are the factors that the government uses in its motion to compel Apple to comply with the court's order.

First, the third party can't be "so far removed from the underlying controversy that its assistance could not be permissibly compelled."[33] For example, in the *New York Telephone* case, the Supreme Court concluded that the district court had found probable cause to believe that the company's facilities were being used to carry out a criminal enterprise. The Court also noted that for the company to refuse to supply the "meager assistance required by the FBI . . . threatened obstruction of an investigation" and the company's assistance would determine whether the phone company's lines were being used illegally.[34] In the Apple case, the government is arguing that Apple is close to the controversy; Apple designed the iPhone, made it, wrote the code, updated the code, and sold the iPhone. Plus, Apple made the *very auto-erase option* that's at issue here.

Second, the writ can't place an unreasonable burden on Apple. Here, the government is arguing, among other things, that because Apple writes code for a living the company can spare an engineer to write code in accordance with the order. But the government is also making it clear that, while the scope of the All Writs Act is broad enough to haul Apple in and make it play ball, the Act doesn't recognize marketing concerns as unreasonable burdens. Interestingly, the government devoted a few pages to arguing that marketing concerns are insufficient grounds to constitute an unreasonable burden. The government's best argument here is that Apple is

[32] Pa. Bureau of Corr., 474 U.S. at 43.

[33] New York Tel. Co., 434 U.S. at 174.

[34] *Id.*

overselling the negative marketing concerns. The order actually lets Apple run the passcode-breaking operation itself at its own facilities—the FBI would remotely send in passcodes and Apple would handle the device.

Third, Apple's assistance must be necessary to effectuate the warrant. (Remember that the phone's owner, Farook's employer, consented to the search and the FBI obtained a warrant.) It's clear here that Apple's assistance is necessary simply because it wrote and built the operating system and code running the device.

VI. CAN THE FBI MAKE SIRI TALK?

In addition to trying to narrow the scope of the All Writs Act, Apple may claim that the court's order *compels* Apple to speak in a way that it doesn't believe in. In short, Apple will likely raise a First Amendment claim. (Of course, that's why they hired Ted Boutrous!)

How this would work makes some sense. Apple doesn't want to write code, code is considered speech,[35] and so Apple is being forced to speak. Code was deemed "speech" in *Bernstein v. United States Department of Justice*. Bernstein, a graduate student at Berkeley, created an encryption equation called "Snuffle." Bernstein wished to publish the algorithm, a paper that described and explained it, and a source code for a computer program that incorporated the algorithm. The Arms Export Control Act and the International Traffic in Arms Regulations required Bernstein to seek the approval of the government and to obtain an export license. After some time, Bernstein challenged the ban on exporting Snuffle. A three-judge panel on the Ninth Circuit concluded that the export regulations as applied to Snuffle—the code—were an impermissible prior restraint on speech.

The First Amendment protects against Congress making laws that abridge the freedom of speech. The First Amendment doesn't say that the courts can't abridge someone's freedom of speech. Would this be a court order that enforces a valid law?

VII. IS PUBLIC PERCEPTION A FACTOR?

Unlike many legal topics that lurk only in dusty law libraries and only concern practitioners steeped in law, privacy law concerns all of

[35] *See* Bernstein v. United States Dep't of Justice, 176 F.3d 1132 (9th Cir. 1997) (holding computer code is protected speech under the First Amendment).

us—lawyers and nonlawyers alike. The outcome of what happens to the San Bernardino shooter's locked iPhone will likely affect a large number of "regular" people.

While the battle over precedents, orders, and appeals will happen in courtrooms, the debate over privacy and the debate over encrypted technology will most surely rage on in the public "town square." Already, we've seen an enormous amount of media coverage on this issue. Tim Cook, Apple's Chief Executive Officer, released a public letter.[36] The appeal to the public doesn't stop there. Jim Comey, the seventh director of the FBI and a former Deputy Attorney General in the George W. Bush administration, wrote a blog post aimed at tamping down anti-government rhetoric.[37] Comey's post tried to frame the issue as narrowly as possible; whereas Cook frames the issue as a civil-liberties one.

Despite the public debate, the action will take place in the courts, and that's why lawyers need to understand what the debate is about, and, perhaps, how it will play out.

VIII. CLOSING

Keep three things in mind as we close here. First, the government will push hard to broaden the scope of the All Writs Act, and Apple will resist this. Second, the government will deny that marketing hits are "unreasonable burdens" and try to narrow the issue to this particular iPhone. And third, Apple may argue that the government violates Apple's First Amendment rights by compelling it to write code.

[36] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[37] James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead*, LAWFARE (Feb. 21, 2016), https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead.