VALLEY LAWYER

JULY 2016 • $4

A Publication of the San Fernando Valley Bar Association

Meet Your 2016 Trustee Candidates

Unlocking Secrets: Public Safety vs. Personal Privacy

Earn MCLE Credit

www.sfvba.org

By reading this article and answering the accompanying test questions, you can earn one MCLE credit. To apply for the credit, please follow the instructions on the test answer form on page 25.

Unlocking Secrets:
Public Safety vs. Personal Privacy

By Adam D.H. Grant

The FBI investigation into December's brutal mass murder in San Bernardino has resulted in a collision between an individual's legal right to privacy and the need to cull information that could well be related to public safety and national security. Although legal action by the U.S. Department of Justice against tech giant Apple to retrieve critical data contained in homegrown terrorist Syed Rizwan Farook's iPhone abruptly ended this spring, the courts will continue to balance public safety with privacy rights as technology evolves.

SINCE TECHNOLOGY GIANT APPLE BURST ONTO the smartphone market with the 2007 launch of the iPhone, the device has come to influence almost every part of our lives. But on February 16, 2016, it also became a national security matter when an iPhone and information it purportedly contained led to a major clash between the U.S. Department of Justice and Apple over the delicate issue of privacy rights.[1]

It all started months before….at a Christmas Party…in an otherwise quiet neighborhood in San Bernardino, California.

Tragic Background

At 10:58 a.m. on December 2, 2015, Syed Rizwan Farook and his wife Tashfeen Malik entered a conference room rented for a training event and holiday party by Farook's employer, the San Bernardino County Department of Public Health (SBCDPH), and unleashed a barrage of bullets that killed 14 people and wounded another 22.

Over time, it became apparent that terrorism had materialized in our own backyard and that Farook's iPhone 5c, the Department of Justice (DOJ) believed, held the key to unlocking critical information that would expose otherwise hidden details as to who exactly had planned the mass murder and how it was facilitated.

Enter Farook's iPhone 5c. At 11:14 a.m., while the shooting was happening, a post appeared on Malik's Facebook page declaring allegiance to ISIS chief, Abu Bakr al-Baghdadi.

Malik and Farook died that afternoon in a gunfight with the police and in the hours and days after the attack, federal, state and local law enforcement agencies conducted over 500 interviews in a concerted attempt to uncover information, not only on motives, but also the identities of third parties who may have assisted in the attack, and where Malik and Farook traveled to and from, before and after the incident.

The critical key to unlocking the secrets they sought, however, were locked in Farook's iPhone 5c, which had been recovered from the couple's car pursuant to a search warrant.

Law enforcement faced two major hurdles in accessing the phone's secrets: the first, easy, the second, unyielding. Farook's employer, SBCDPH, owned the phone and assigned it to him as part of its "Corporate Owned, Personally Enabled," or COPE program, through which an employer provides cell phones, among other devices, to be used and managed for business purposes by its employees.

Employers implement this program because it provides the employer more control over communications devices their employees use during the course of their work. As Farook's employer implemented the COPE program, law enforcement was obligated to obtain SBCDPH's authorization to conduct a forensic examination of the phone. Permission to examine Farook's iPhone was requested and readily obtained from the agency.

Additionally, Farook's employer had a written policy as part of its COPE program which allowed it to search all agency-issued digital devices at any time. This is a common practice in California, which invalidates most claims by employees that they have an expectation of privacy while using an employer-provide telecommunications device.

U.S. Attorney's Office Seeks the Ultimate Order

In time, though, Apple, which developed both the iPhone and its operating software, proved to be the unyielding hurdle. According to the ex parte application filed by the U.S. Attorney's Office on February 16, 2016:

> *"Despite the search warrant and the owner's consent, the FBI has been unable to search the subject device because it is 'locked' or secured with a user-determined, numeric passcode. More to the point, the FBI has been unable to make attempts to determine the passcode because Apple has written, or 'coded,' its operating system with a user-enabled 'auto-erase function' that would, if enabled, result in the permanent destruction of the required encryption key material after 10 erroneous attempts at the passcode."*

Simply, after ten failed attempts at inputting the passcode, Apple protocols call for data on the device to become permanently inaccessible. At the request of the U.S. Attorney's Office, Apple made itself available 24/7 to assist with the investigation, until it was, in its opinion, asked to develop an entirely new iPhone operating system.

Apple refused the request and, on February 16, 2016, the U.S. Attorney's Office filed a motion for an order "to assist in the execution of a search warrant using the

Adam D. H. Grant is is a partner with the law firm of Alpert, Barr & Grant in Encino. An experienced trial lawyer, he has considerable litigation experience in online privacy and business issues. He can be reached at agrant@alpertbarr.com.

capabilities that Apple has retained along with its encryption software, so the government can attempt to determine the passcode without the additional, non-encryption features that Apple has coded into its operating system, for the subject device only."

The DOJ specifically sought an order that Apple must provide the FBI with a custom iPhone software file which would allow the agency to bypass the auto-erase function and access the data on Farook's cell phone.

U. S. Attorney's Office Tries Everything in Its Quiver

The government's first argument rested on the most sweeping discretionary law applicable. The All Writs Act, according to the motion, "allows 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."[2]

According to the U.S. Supreme Court decision in *Pennsylvania Bureau of Correction v. United States Marshals Service*,[3] "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute,"[4] while the Ninth Circuit, the ever present leader in application of the law to the technology, has held that a court has the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers."[5]

The U.S. Attorney also relied on a New York case in which it a court required a manufacturer to assist in accessing a cell phone's files so that a warrant may be executed as originally contemplated.[6]

> "A federal magistrate judge ruled that the government can compel a cell phone manufacturer to help unlock a password-protected device to enable police to execute a search warrant."

The motion and the citation to the timely order did not tell the entire story. A federal magistrate judge from the U.S. District Court for the Southern District of New York ruled that the government can compel a cell-phone manufacturer to help unlock a password-protected device to enable police to execute a search warrant. However, the magistrate judge inserted a key proviso which the DOJ did not address in the *ex parte* application. The magistrate approved the order, but cautioned that the manufacturer must be provided an opportunity to dispute the order if compliance with the order would be "unreasonably burdensome."[7]

According to the *ex parte* application, "Apple has the ability to modify software that is created to only function within the subject device that would ensure the auto-erase function is turned off, allow for electronic submission of test passcodes, and ensure additional delays are not created." However, it would seem that the DOJ forgot not just one, but two very critical points when it filed the ex parte application.

Magistrate Judge of the Central District of California Sheri Pym granted the application and entered the order on February 16, 2016, without Apple being given an opportunity to file an opposition. Judge Pym granted the application as requested, but, in keeping with the language of the New York magistrate's prior order, she included a caveat in the order: "To the extent that Apple believes that compliance with this order would be unreasonably burdensome, it may make an application to this Court for relief within five business days of receipt of this order." Thus, Judge Pym left the door wide open for Apple to demonstrate why the order would be unreasonably burdensome.

Champion of Privacy and Defender of Its Rights

On February 25, 2016, Apple filed a Motion to Vacate the order compelling it to assist the FBI and the Department of Justice and oppose the government's Motion to Compel Assistance. At the outset of the Motion to Vacate, Apple appeared to champion the cause for the "basic security and privacy interests of hundreds of millions of individuals around the globe." Additionally, it framed the issues around its request to "create a back door to defeat the encryption on the iPhone, making to its users' most confidential and personal information vulnerable to hackers, identify thieves, hostile foreign agents, and unwarranted government surveillance."

Apple then countered the Department of Justice's reading of the All Writs Acts by arguing that it "does not give the district court a roving commission to conscript and commandeer Apple..." Additionally, Apple defined the two key components of the case, namely the needs of law enforcement, and the privacy and personal safety interest in the public, and addressed what is, in its opinion, the heart of the motion, the government's blunder and the unduly burdensome nature of the order itself.

Apple also reminded the Department of Justice that it rapidly responded to all the FBI's requests, but pointed out that the Department failed to consult with Apple on a key issue. Apparently, the FBI, without talking with Apple or reviewing Apple's public guidance regarding its operating

system, changed the iCloud password associated with one of the attacker's accounts. As a result, the FBI, according to Apple, foreclosed "the possibility of the phone initiating an automatic iCloud back-up of its data to a known Wi-Fi network, which could have obviated the need to unlock the phone and thus for the extraordinary order the government now seeks." Apple asserted that if the FBI had simply asked Apple first, the entire litigation would not have been necessary.

Apple then walked through Magistrate Judge Pym's "open door" regarding the ability to challenge the order on the ground that it was "unduly burdensome." According to Apple, "[t]he software envisioned by the government simply does not exist today." As the company saw it, the government was forcing it to create a new version of the iPhone operating system to circumvent a very important security feature.

Apple estimated it would take a team of computer engineers up to a month to create a new operating system (OS) that would meet the company's exacting quality control standards and require an even more comprehensive level of testing and analysis. In addition, Apple's quality assurance department would need to insure that the new OS would not inadvertently destroy or alter any existing user data. The company clearly demonstrated that it fell within the "unduly burdensome" prong—specifically since the government mistakenly changed the iCloud password and, thus, set the entire legal process in motion.

Apple's Motion to Vacate attacks the very heart of the Department of Justice's heavy reliance on *United States v. Telephone Co*.[8] Apple focused on the fact that the District Court in the New York Telephone Co. case merely ordered the company to install a pen register (a simple device designed to record dialed numbers) on two telephones. The company noted that the Court found the order had complied with a three part test—first, the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled";[9] *second*, the assistance needed was meager and the company did not have a substantial interest to not provide the assistance;[10] and third, there was no conceivable way the surveillance could have been successful without the company's assistance.[11] Apple then applied the test to the facts of its case and easily concluded that the court should reverse its prior order.

Abrupt End to a Bitter Dispute

Shortly after the maelstrom of legal wrangling made headlines around the world, the entire dispute came to an abrupt halt. One day before the scheduled March 22, 2016 hearing on the Motion to Vacate, the court ordered the government to provide a status report.

Six days later, the Department of Justice filed a report which succinctly stated that, "[t]he government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by the court's February 16, 2016, order compelling Apple to

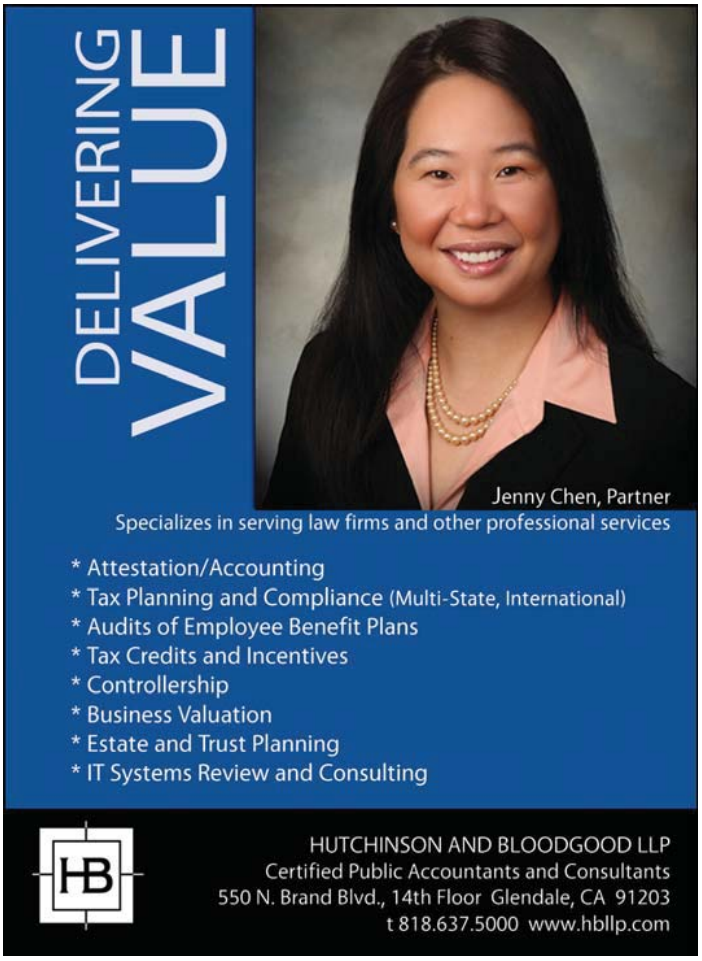
I am pleased to announce my new association with

Dilbeck Real Estate

Please feel free to call me if I can be of assistance to you in any aspect of real estate.

Steven M. West
Broker Associate
CalBRE# 02000607
Direct: 818.755.5559
Cell: 818.808.3179
Steven.West@dilbeck.com
StevenWest.dilbeck.com

12164 Ventura Boulevard, Studio City, CA 91604



Hot Writs & Cool Appeals

Herb Fox, Esq.
Certified Appellate Law Specialist*
A Full Service Appellate Boutique

Former Research Attorney, State Court of Appeal

29 Years Experience

250+ Appeals and Writs of Record

Appeals and Writs

Petitions for Review and Certiorari

Post-Trial and Anti-SLAPP Motions

Appellate Opinion Letters

Pre-Trial, Trial, and Post-Trial Consultations

310.284.3184
HFox@FoxAppeals.com
www.FoxAppeals.com

Hourly, Flat and Contingency Fees Considered
Referral Fees Paid in Accordance with State Bar Requirements

Southern California Appellate Superlawyer©
AV© Rated / AVVO© Rating 10

**Board of Legal Specialization, Cal. State Bar*

assist its agents conducting the investigation. Since the status report was filed, Apple has requested information on the identity of the unidentified third party who assisted the FBI, as well as technical details of the computer procedures developed to access the data, a development that may well morph into a major privacy battle in 2016.

What Is So Important about an iPhone?

After all the legal maneuvering, the real question is why would such a case garner such worldwide attention? Why is the data stored in an iPhone so important? The answer is likely contained in a United Supreme Court Case Apple cited in its opposition, *Riley v. California*.[12]

On June 25, 2014, the Supreme Court issued its opinion in the case, which addressed the question whether the police properly searched Riley's mobile phone as part of a routine traffic stop. The officer accessed information on the phone and noted the repeated use of a term that the police associated with street gang activity. A detective specializing in gangs examined the phone's digital contents and based in part on the photos and videos the detective found on the device, later charged Riley in an earlier gang-related shooting with a recommendation for an enhanced sentence based on his gang membership.

Riley moved to suppress all of the evidence the police obtained from his cell phone. The trial court denied the motion and Riley was convicted. The Court of Appeals affirmed the denial and the conviction. The Supreme Court, however, reversed the judgment and remanded the case to the trial court.

The *Riley* decision is germane to the Apple case because of the Court's recognition of how ubiquitous the cell phone has become in our everyday activities and how such telecommunications technology has impacted the law and its interpretation.

The decision includes an extensive discussion of privacy rights associated with data stored on virtually everyone's mobile phone. In announcing the decision, Chief Justice Roberts observed that cell phones "are now 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."[13] Further, in rejecting the government's assertion that searching for data stored on a cell phone is materially indistinguishable from searches of a person's physical items, Roberts retorted, "[t]hat is like saying a ride on a horseback is materially indistinguishable from a flight to the moon."[14]

The Court's analysis regarding warrantless searches spanned 40 years. In *Chimel v. California*,[15] when analyzing a warrantless search of a home, the Court laid the groundwork for the current search incident to arrest doctrine. The Court concluded that "[w]hen an arrest is made, it is reasonable

for the arresting officer to search the person arrested in order to remove any weapon that the latter might seek to use in order to resist arrest or effect his escape."[16] In *United States v. Robinson*,[17] the Court turned its attention to a warrantless search of the arrestee's person. In concluding the search was reasonable, the court explained that, "[t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect."[18]

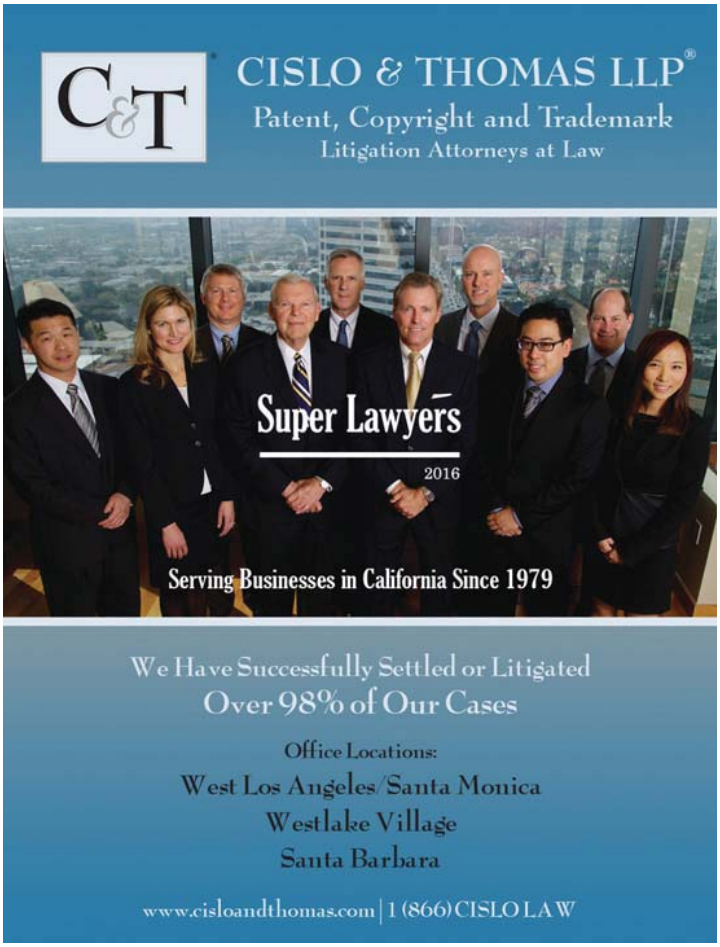
Finally, the Court in *Arizona v. Gant*[19] recognized that the concerns for officer safety and evidence preservation expressed in the *Chimel* decision underline the search incident to the arrest exception. However, the Court allowed a warrantless search of a vehicle's passenger compartment "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."[20] Using this trilogy of cases as the backdrop, the *Rley* Court made several interesting observations. First, it declared that the data stored on a cell phone "cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[21]

It's interesting to note here that a certain mobile application (or app) can be used to broadcast a "panic" alert to pre-determined recipient's emails via a text message as to the location of a person and his/her immediate need. Taking it one step further, it's not difficult to imagine the app being used to broadcast to other criminals an arrestee's exact location and a message indicating that he was being detained by the police. Clearly such information could be used to thwart an arrest or actually create a threat to the arresting officers.

The Court further opined that once police offers secure a cell phone, "there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."[22] But, in fact, another app is configured to erase all data from a cell phone when it loses its connection with blue tooth-enabled hardware that is tethered to the phone.

The Court recognized a key component to the issue of privacy, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person,"[23] noting that cell phones have the capacity to hold an immense amount of data, including photos, videos, addresses, bank statements or medical information accumulated over a period of years.

Most notable was the Court's discussion of the use of mobile apps with cell phones. The *Riley* Court recognized that "the average smart phone user has installed 33 apps on his phone, which can combine to form a revealing montage of the cell phone owner's life."[24] The Court even recognized there are more than a million apps available in each of the two major app stores.



WHY FIGHT TRAFFIC TO GET OVER THE HILL FOR A FEE DISPUTE?

Resolve your matter easily through the San Fernando Valley Bar Association's Mandatory Fee Arbitration Program.

The Mandatory Fee Arbitration Program offers a neutral, efficient and cost-effective forum for resolving attorney-client fee disputes. Through the Mandatory Fee Arbitration Program, your disputes can be resolved quickly and confidentially by local arbitrators.

THE MANDATORY FEE ARBITRATION OFFERS

- Qualified attorney and lay arbitrators
- Confidential hearings
- A quick and less expensive alternative to court

Mandatory Fee Arbitration PROGRAM

San Fernando Valley Bar Association

Visit *www.sfvba.org* for more information or contact Program Administrator Melissa Garcia at (818) 227-0490, ext. 107 or melissa@sfvba.org.

In the end, the Court ruled that given the immense quantity and quality of information stored on the average person's cellphone, the intrusion into a person's privacy is far greater than any legitimate governmental interest in searching the data stored on the phone incident to an arrest. The court specifically left open the possibility of a warrantless search if it was presented with evidence of exigent circumstances which were not present in this particular arrest.

A recent article in the *Wall Street Journal*[25] touched on what might likely be the next intersection of technology and the law—wearable technology and the workplace. The article addressed the question of how companies should handle data gleaned from an employee utilizing a wearable device. The article recognized that tracking an employee's whereabouts and work habits can trigger a number of privacy issues by raising the issue of disclosure and the use of the data collected, as well as whether an employer can require employees to wear such devices.

The recognition that intrusion into the data stored on a person's cell phone is greater than evidence located in a person's home will undoubtedly be used in the future to strengthen privacy laws and increase the use of privacy notices. Additionally, an appreciation of the quality of information and the ability to create personally identifiable information from non-identifying sources will likely lead to the expansion of the need to properly disclose when certain information is obtained and what the information will be used for by the company.

As technology evolves, cell phones and other communications devices will likely unlock many secrets that run the gamut from exposing a terrorist's communications with his cohorts to how often someone visits their office water cooler. Only time will tell.

---

[1] *In the Matter of the Search of an Apple iPhone*, United States District Court Case No. 15-0451M.
[2] 28 U.S.C. Section 1651(a).
[3] 474 U.S. 34 (1985).
[4] *Id.* 43.
[5] *Plum Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979).
[6] In re Order Requiring [xxx], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone No. 14 Mag. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014).
[7] *Id.* at *3.
[8] 434 U.S. 159 (1977).
[9] *Id.* at 174.
[10] *Id.*
[11] *Id.* at 175.
[12] 134 S.Ct. 2473 (2014).
[13] *Id.* at 2484
[14] *Id.* at 2488
[15] 395 U.S. 752 (1969).
[16] *Id.* at 763.
[17] 414 U.S. 218 (1973).
[18] *Id.* at 235.
[19] 556 U.S. 332 (2009).
[20] *Id.* at 335.
[21] *Riley*, 134 S.Ct. at 2478.
[22] *Id.* at 2486.
[23] *Id.* at 2489.
[24] *Id.* at 2490.
[25] "*Should Law Enforcement Have to Get a Warrant to Obtain Stored Emails," Wall Street Journal, May 22, 2016*.