CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Essay

Social Justice and Silicon Valley: A Perspective on the Apple-FBI Case and the "Going Dark" Debate

MAJ. GEN. CHARLES J. DUNLAP, JR., USAF (RET.)

ESSAY CONTENTS

Social Justice and Silicon Valley: A Perspective on the Apple-FBI Case and the "Going Dark" Debate

MAJ. GEN. CHARLES J. DUNLAP, JR., USAF (RET.)*

INTRODUCTION

Social justice, we are told, "is generally equated with the notion of equality or equal opportunity in society."[1] It also embraces the idea of economic justice.[2] This essay argues that these concepts are involved in last year's dispute between Apple Inc. and the Federal Bureau of Investigation (FBI) over an encrypted phone found among the possessions of one perpetrator of the San Bernardino massacre that killed fourteen people and wounded twenty-two.[3]

The phone was believed to be evidence in a terrorism case, and the FBI received permission from the owner of the phone (the San Bernardino County Department of Public Health) to search its content. They were stymied, however, by the Apple phone's encryption software that effectively "locked" the phone. The FBI then obtained a court order under the All Writs Act[4] compelling Apple's assistance in unlocking the phone, but the corporation resisted doing so.[5] The Department of Justice eventually dropped the case against Apple when the FBI gained access to

---

* Maj. Gen. Charles J. Dunlap, USAF (Ret.) is a Professor of the Practice of Law and Executive Director of the Center on Law, Ethics and National Security at Duke University School of Law. The author wishes to thank the many members of the *Connecticut Law Review* whose very significant efforts made this essay possible.

[1] Allan Scherlen & Matthew Robinson, *Open Access to Criminal Justice Scholarship: A Matter of Social Justice*, 19 J. CRIM. JUST. EDUC. 54, 62 (2008).

[2] *Defining Economic Justice and Social Justice*, CTR. FOR ECON. & SOC. JUST., http://www.cesj.org/learn/definitions/defining-economic-justice-and-social-justice/ [https://perma.cc/UC4G-GVN7] (last visited Jan. 26, 2017).

[3] For general background, see Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html [https://perma.cc/ALL3-MDPH]; *Everything We Know About the San Bernardino Terror Attack Investigation So Far*, L.A. TIMES (Dec. 14, 2015, 4:03 PM), http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html [https://perma.cc/MQ3A-6YWR] (providing information on the San Bernardino terror attack investigation).

[4] 28 U.S.C. § 1651 (2012).

[5] *See* Kharpal, *supra* note 3 ("The judge asked Apple to provide 'reasonable technical assistance' to the U.S. authorities, which would require the technology giant to overhaul the system that disables the phone after 10 unsuccessful password attempts. Once this feature kicks in, all the data on the phone is inaccessible. Apple declined to help the FBI.").

the phone with the help of a third party.[6]

Nevertheless, the dispute highlights what has been called the "going dark" debate, where technology is frustrating the ability of law enforcement to investigate crimes and national security threats, even where the government is working through the judiciary.[7] Apple's contention that "nothing is more important than the safety of all of our customers"[8] is juxtaposed against the FBI's broader mission to "protect the American people"[9] in general (and not just Apple customers), as well as the Supreme Court's admonition in *Haig v. Agee*[10] that "no governmental interest is more compelling than the security of the Nation."[11]

While Apple argued that the main dispute was one about individual privacy rights against government intrusion, in truth, it engages fundamental notions of social justice and the rule of law. This Essay suggests several key questions. First, in a free society, to what extent should Silicon Valley—as opposed to the courts—determine what law enforcement professionals can and cannot do, particularly when the tech moguls making that determination have the wealth to insulate themselves from the consequences of their decisions?[12]

Additionally, if commercial companies believe that encryption is vital to the viability of their brand, should they nevertheless bear the costs when their devices enable the commission of criminal acts and terrorism? Should a statutory presumption be established to benefit victims where a

---

[6] Laurie Segall et al., *FBI Says It Has Cracked Terrorist's iPhone Without Apple's Help*, CNNMONEY (Mar. 29, 2016, 9:36 AM), http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/ [https://perma.cc/TU4C-4SKD].

[7] *See* KRISTIN FINKLEA, CONG. RESEARCH SERV., R44481, ENCRYPTION AND THE "GOING DARK" DEBATE 1 (2016) ("[S]ome posit that law enforcement is 'going dark' as their investigative capabilities are outpaced by the speed of technological change. As such, law enforcement cannot access certain information they otherwise may be authorized to obtain."); *Apple vs. the FBI: The Complete Guide*, BLOOMBERG, https://www.bloomberg.com/news/special-reports/apple-fbi-encryption-standoff [https://perma.cc/JQ3K-7XWV] (last visited Jan. 25, 2017) (providing different perspectives on the ongoing debate over "encryption, privacy, and the iPhone").

[8] Craig Federighi, Opinion, *Apple VP: The FBI Wants to Roll Back Safeguards That Keep Us a Step Ahead of Criminals*, WASH. POST (Mar. 6, 2016), https://www.washingtonpost.com/opinions/apple-vp-the-fbi-wants-to-roll-back-safeguards-that-keep-us-a-step-ahead-of-criminals/2016/03/06/cceb0622-e3d1-11e5-a6f3-21ccdbc5f74e_story.html?utm_term=.d7607a35734f [https://perma.cc/P7EM-CX5H].

[9] *Mission & Priorities*, FBI, https://www.fbi.gov/about/mission [https://perma.cc/7P5Z-8PYD] (last visited Feb. 20, 2017).

[10] 453 U.S. 280 (1981).

[11] *Id.* at 307.

[12] *See* Evan Osnos, *Doomsday Prep for the Super-Rich*, NEW YORKER (Jan. 30, 2017), http://www.newyorker.com/magazine/2017/01/30/doomsday-prep-for-the-super-rich [https://perma.cc/9WZA-Z2F3] (discussing how "[s]urvivalism, the practice of preparing for a crackup of civilization . . . [has] in recent years . . . expanded to more affluent quarters, taking root in Silicon Valley and New York City, among technology executives, hedge-fund managers, and others in their economic cohort").

reasonable inference is established that a phone or similar device was used by the perpetrator of a crime or terrorist act where the company involved either designed it with "unbreakable" encryption or refuses to aid in its decryption despite a court order?

Along these lines, in a nation where courts have traditionally resolved the inherent tension between privacy and security, are we seeing adjudication, de facto, shift to private entities with a commercial interest in the outcome? Does former Director of the CIA John Brennan raise a legitimate concern when he says, in reference to the Apple-FBI case, that:

> So . . . if a judge issues a writ that says a safety deposit box in a bank must be opened up because there's something in there either inculpatory, exculpatory of the crime or something that's going to allow us to prevent a crime, the bank owner has a legal obligation to open it up. Same thing with a warehouse owner, or somebody who owns an apartment building. *Now private sector companies are getting the ability to say to the government and to the courts and to our system of laws, no, I'm going to determine what the government is going to be able to see or not*[?][13]

Moreover, in a free enterprise system, to what extent should the legitimate financial interests of private companies[14]—not to mention the bona fide individual interests and rights of the *customers* of that company—prevail over the security interests of the public at large, to include those whose financial means are such that they must depend upon government for protection as the wealthy do not?[15] How much privacy and civil liberty does the public want to forfeit in a technological era that Thomas Friedman tells us is enabling even *individuals* to become what he calls "super-empowered" individuals to "kill all of us"?[16] Is he correct when he says, "[W]e need to ensure our government has all the

---

[13] JOHN BRENNAN, A CANDID CONVERSATION WITH THE DIRECTOR OF THE CIA, INTERVIEW AT THE ASPEN SECURITY FORUM 22 (Jul. 29, 2016), http://aspensecurityforum.org/wp-content/uploads/2016/07/a-candid-conversation-with-the-director-of-the-cia.pdf [https://perma.cc/XFD3-XQ9P] (emphasis added).

[14] David Goldman, *Apple's iPhone Sales Sink for the First Time Ever Last Quarter*, CNN (Apr. 26, 2016, 5:45 PM), http://money.cnn.com/2016/04/26/technology/apple-earnings/ [https://perma.cc/7SN4-E68S].

[15] *See, e.g.*, Ian Mohr, *Mark Zuckerberg Hired 16 Bodyguards to Protect Him at Home*, PAGE SIX (Feb. 14, 2016, 10:30 PM), http://pagesix.com/2016/02/14/mark-zuckerberg-has-16-bodyguards-at-his-home/ [https://perma.cc/T3P5-EV7F] (reporting that "young tech billionaires" like Mark Zuckerberg can afford their own security details to protect them from "threats from unstable users").

[16] *See* Thomas L. Friedman, Opinion, *Lessons of Hiroshima and Orlando*, N.Y. TIMES (June 15, 2016), https://www.nytimes.com/2016/06/15/opinion/lessons-of-hiroshima-and-orlando.html?_r=0 [https://perma.cc/L6M9-NNNV] ("[W]e're entering a world where small groups—maybe even soon a single super-empowered person—will be able to kill all of us . . . .").

surveillance powers it needs—under appropriate judicial review—to monitor and arrest violent extremists of all stripes. *The bad guys now have too many tools to elude detection*"?[17]

At the same time, however, we need to keep in mind, as Mieke Eoyang has pointed out, that "[t]he debate is often framed as a balance between government power and individual privacy."[18] Eoyang says this too often overlooks the "critical role of the communications companies, who as physical and legal gatekeepers regulate government access to private information."[19] She also states that "when the government does not properly balance the economic concerns with the national security concerns it can harm U.S. competitiveness abroad."[20]

The purpose of this short Essay is not to dissect the technicalities of the Apple-FBI litigation, but rather to argue that in a democracy, there will always be tensions between privacy and security. And in resolving such tensions, social justice would call for a better accounting of the needs of those who are not customers of a particular commercial entity and who cannot depend for security upon their own resources, but rather must look to law enforcement and government for protection.

I. CONTEXT

The Apple-FBI dispute resulted from a tragic December 2015 attack by Syed Rizwan Farook and his wife, Tashfeen Malik, in San Bernardino, California, in which fourteen people were killed and twenty-two were injured in what has been called "a vicious and premeditated terrorist attack."[21] Farook and Malik were later killed in a shootout with police.[22]

In the investigation that followed, a search pursuant to a warrant of Farook's vehicle produced a cell phone belonging to his employer, the San

---

[17] *Id*. (emphasis added).

[18] Mieke Eoyang & David Forscey, *Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic Surveillance*, LAWFARE (Apr. 11, 2016, 7:22 AM), https://www.lawfareblog.com/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance-0 [https://perma.cc/262R-9QZU].

[19] *Id.*

[20] Mieke Eoyang, *Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance* 5 (Hoover Inst., Aegis Paper Series No. 1603, Apr. 8, 2016), http://www.hoover.org/sites/default/files/research/docs/eoyang_privacysecurity_final_v3_digital.pdf [https://perma.cc/63PW-4FBW].

[21] RICK BRAZIEL ET AL., CRITICAL RESPONSE INITIATIVE, OFF. OF CMTY. ORIENTED POLICING SERVS., U.S. DEP'T OF JUST., BRINGING CALM TO CHAOS: A CRITICAL INCIDENT REVIEW OF THE SAN BERNARDINO PUBLIC SAFETY RESPONSE TO THE DECEMBER 2, 2015, TERRORIST SHOOTING INCIDENT AT THE INLAND REGIONAL CENTER ix (2016), https://www.justice.gov/usao-cdca/file/891996/download [https://perma.cc/3HFC-RM63].

[22] *See id.* at 39–40 (explaining the gunfight and the manner in which the assailants were shot by police).

Bernardino County Department of Health.[23] What happened next is explained in the government's later application to the court:

> In the hopes of gaining crucial evidence about the December 2, 2015 massacre in San Bernardino, California, the government has sought to search a lawfully-seized Apple iPhone used by one of the mass murderers. Despite both a warrant authorizing the search and the phone owner's consent, the government has been unable to complete the search because it cannot access the iPhone's encrypted content. Apple has the exclusive technical means which would assist the government in completing its search, but has declined to provide that assistance voluntarily. Accordingly, the government respectfully requests that this Court issue an order compelling Apple to assist in enabling the search commanded by the warrant.[24]

The government needed Apple's technical assistance because the phone's software was such that the government was unable to "unlock" the phone without risking the destruction of whatever data it might have held.[25] The court issued an order to Apple compelling their cooperation,[26] but Apple resisted the court's motion.[27] Nevertheless, before there was any definitive resolution, the government ended the litigation when it advised the court it had "successfully accessed the data stored on Farook's iPhone

---

[23] Government's Motion to Compel Apple Inc. to Comply with this Court's Feb. 16, 2016 Order Compelling Assistance in Search at 5, *In re* 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, 2016 WL 618401769612 (C.D. Cal. Feb. 19, 2016).

[24] Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search at 3, *In re* 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, 2016 WL 618401 (C.D. Cal. Feb. 19, 2016).

[25] Government's Motion to Compel, *supra* note 23, at 5 ("Nonetheless, despite the search warrant ordered by the Court and the owner's consent to search the SUBJECT DEVICE, the FBI has been unable to search [it] 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 to access the [device] because Apple has written, or 'coded,' its operating systems with a user-enabled 'auto-erase function' that would, if enabled, result in the permanent destruction of the required encryption key material after 10 failed attempts at entering the correct passcode.").

[26] *In re* 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, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016) (order compelling Apple, Inc. to assist agents in search).

[27] *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?postshare=9501485386886260&tid=ss_mail&utm_term=.72ab40da8569 [https://perma.cc/A26U-HRSV] (explaining Apple's decision to fight federal demands).

and therefore no longer require[d] the assistance from Apple Inc."[28]

II. THE APPLE STRATEGY

Apple always wanted to portray its case in a way that postured itself as the defender of privacy and personal safety versus an Orwellian government, but it is really more about a mammoth corporation's interests versus the rule of law and the people who do not happen to be their customers or, if they are their customers, people without the resources of those who would most benefit financially from the ability to sell a "law enforcement proof" communications device.

Apple engaged in a well-conceived and well-executed public relations campaign to propagate its view of the dispute. In a February 16, 2016 letter to customers, Apple CEO Tim Cook characterized the FBI's court order as a threat to privacy which would "undermine the very freedoms and liberty our government is meant to protect."[29] Similarly, the company's Vice President, Craig Federighi, wrote an op-ed claiming that "nothing is more important than the safety" of Apple customers.[30] Essentially, Apple argued that "if it were to weaken the encryption on one phone, the encryption on all phones of that type would be weakened, too."[31]

According to Apple, the decryption "would in effect create an opening through which some clever bad apple could wreak all kinds of chaos."[32] In other words, Apple's announced focus was on its customers. Quite obviously, the FBI would be concerned not just with those who choose to be Apple's customers, but rather with the citizenry writ large, to include those who elect not to be customers either by choice or by the absence of financial resources. In addition, there are the interests of those for whom the privacy value of an encrypted phone, whether theirs or another's, does not outweigh the desire to be protected from the mayhem of those whose illicit activities would be facilitated by the technology.

The FBI did try to counter Apple's hype and temper public concerns: former FBI Director James Comey said law enforcement "simply want[s]

---

[28] Government's Status Report at 1, *In re* 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 (C.D. Cal. Mar. 28, 2016); *see also* Proposed Order Vacating Feb. 16, 2016 Order, *In re* 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 (C.D. Cal. Mar. 28, 2016) ("The Court has reviewed the government's Status Report . . . the Court hereby [vacates] the Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016.").

[29] Letter from Tim Cook, CEO, Apple, to Customers (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/CER6-45KL].

[30] Federighi, *supra* note 8.

[31] Mark Sullivan, *Where Will Trump Fall on the Encryption Debate? Tough Call*, FAST CO. (Dec. 29, 2016, 3:00 PM), https://www.fastcompany.com/3066637/tech-forecast/where-will-trump-fall-on-the-encryption-debate-tough-call [https://perma.cc/CW5D-LPT5].

[32] *Id.*

the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it."[33]

But Apple's advocacy efforts enjoyed real success. Although initially polls showed that the majority of Americans supported the FBI over Apple, they later showed the public to be split more evenly.[34] This led many, like commentator Mark Sullivan, to conclude that "Apple eventually won the PR war, successfully spreading the message that weakening encryption hurts everybody and works against both national security and law enforcement interests."[35]

III. THE FINANCIAL FACTOR

Despite the way Apple presented its case, it is clear that it had interests beyond the stated fear that "the very freedoms and liberty our government is meant to protect" were in jeopardy.[36] Specifically, it is apparent that Apple was under real financial pressure at the time the San Bernardino case arose. In April 2016, the corporation reported "its worst quarter in over a decade."[37] More specifically as to the devices in the Apple-FBI case, CNN said "iPhone sales fell for the first time in history."[38] This is critical for Apple because "more than two-thirds of Apple's revenue is made up of iPhone sales."[39] Consequently, CNN's David Goldman concludes that "where the iPhone goes, so goes Apple."[40]

Early on, the *New York Times* suggested that there were factors of impersonal corporate interests at play in the case. The *Times* said:

> The company is playing the long game with its business. Privacy and security have become part of its brand, especially internationally, where it reaps almost two-thirds of its almost $234 billion a year in sales. And if it cooperates with one government, the thinking goes, it will have to

---

[33] James B. Comey, *We Could Not Look the Survivors in the Eye If We Did Not Follow This Lead*, LAWFARE (Feb. 21, 2016, 9:03 PM), https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead [https://perma.cc/TSJ9-RKQW].

[34] Ben Lovejoy, *WSJ/NBC Poll Shows Public Support for Apple's Side of FBI Battle Growing, Now Close to Even Split*, 9TO5MAC (Mar. 9, 2016 4:07 AM), https://9to5mac.com/2016/03/09/apple-fbi-public-poll-2/ [https://perma.cc/LR9W-K67M].

[35] Sullivan, *supra* note 31.

[36] Cook, *supra* note 29.

[37] Goldman, *supra* note 14.

[38] *Id*.

[39] *Id*.

[40] *Id*.

> cooperate with all of them.[41]

Businessman Blair Reeves made this point unequivocally:

> For several years now, Apple has explicitly made "privacy" a key marketing stick with which to beat its chief competitor, Google. Certainly, a stated commitment to protect customer privacy is vital to Apple's brand and continuing business strategy. Apple's CEO and employees may be expressing genuinely held private convictions, but the regulatory theater in which Apple, the corporation, is currently embarked is without question motivated by its business concerns.[42]

Of course, Silicon Valley, one of the greatest concentrations of extreme wealth on the planet,[43] rallied to support Apple, seeming to forget that while they can hire armies of bodyguards and other security,[44] the bulk of the citizenry is vastly more vulnerable to those terrorists and criminals who will exploit any inability of law enforcement and the courts to penetrate their communications. The Silicon Valley billionaires seem to be forgetting that the reason they have made all their money is that they are privileged to live in a country with robust policing and a strong judiciary.

In addition, Apple makes two thirds of its sales overseas including some $59 billion in China.[45] The *Los Angeles Times* suggested that Apple was trying to calm the national security concerns of the Chinese government, while making accommodations, such as storing data on

---

[41] Katie Benner & Paul Mozur, *Apple Sees Value in Its Stand to Protect Security*, N.Y. TIMES (Feb. 20, 2016), https://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html?_r=2 [https://perma.cc/86W7-AN9Q].

[42] Blair Reeves, *Demystifying Apple's FAQ—A Rebuttal*, LAWFARE (Feb. 29, 2016, 12:24 PM), https://www.lawfareblog.com/demystifying-apples-faq-–-rebuttal [https://perma.cc/AMJ9-2P5A].

[43] *See* Rich Robinson, *Silicon Valley: Richest Region in America Can, Must Do Better*, SAN JOSE INSIDE (Oct. 20, 2015), http://www.sanjoseinside.com/2015/10/20/silcion-valley-richest-region-in-america-can-must-do-better/ [https://perma.cc/62T3-PH8M] (noting that the San Jose-Sunnyvale-Santa Clara metro area's median household income is the highest in the United States); Josie Ensor, *Silicon Valley Mints 23 New Billionaires to Become Best Place to Get Rich*, TELEGRAPH (Mar. 3, 2015, 12:28 AM), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11446029/Silicon-Valley-mints-23-new-billionaires-to-become-best-place-to-get-rich.html [https://perma.cc/J2QJ-RZVD] (noting that Silicon Valley is "home to the greatest number of billionaires on the planet after China and the U.S.").

[44] *See* Mohr, *supra* note 15 ("Insiders tell Page Six that the young tech billionaires are forced to hire armies of guards after threats from unstable users.").

[45] *See* David Pierson, *While It Defies U.S. Government, Apple Abides by China's Orders—and Reaps Big Rewards*, L.A. TIMES (Feb. 26, 2016, 3:00 AM), http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html [https://perma.cc/PMV2-QB9Z] (noting that sales of Apple products in the greater China region reached $59 billion last year); *Non-U.S. Share of Apple's Revenue from 1st Quarter 2006 to 1st Quarter 2017*, STATISTA, https://www.statista.com/statistics/263435/non-us-share-of-apples-revenue/ [https://perma.cc/FPU9-RF2M] (last visited Apr. 20, 2017) (showing that 64% of Apple's revenue in the first quarter of 2017 came from outside of the U.S.).

vulnerable servers in China.[46] The *Times* quoted James Lewis, senior fellow at the Center for Strategic and International Studies in Washington, who said:

> "What's driving this is Apple's desire to persuade the global market, and particularly the China market, that the FBI can't just stroll in and ask for data . . . . I can't imagine the Chinese would tolerate end-to-end encryption or a refusal to cooperate with their police, particularly in a terrorism case."[47]

In short, Apple is—and has been—monetizing the value of privacy to reinforce its brand in the marketplace. There is nothing unlawful, per se, about a commercial interest in doing just that; this issue is to what extent—if any—should that be limited.

IV. TRADE OFFS

A couple of things need to be made clear. In the first place, in a free-enterprise system, there is nothing illegal about a corporation seeking to maximize its profits within the law. Indeed, there is much to be said about the idea that competition in the marketplace injects an efficiency into commerce that inures to the benefit of all. At the same time, however, the untamed pursuit of profits has proven itself to be, at times, detrimental to the society at large. For this reason, there are times when government intervention is prudent and necessary.

One of those instances arises in resolving the inherent tension between the value of a corporate quest for profits in a free-enterprise system, and the interests of government in the security of the people. As to the latter, the Supreme Court in *Haig v. Agee* observed that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[48]

Interestingly, Apple implicitly argued that even that imperative has its limits. In its March 22, 2016 motion it said:

> However, while the government's desire to maximize security is laudable, the decision of how to do so while also protecting other vital interests, such as personal safety and privacy, is for American citizens to make through the democratic process. Indeed, examples abound of society

---

[46] *See Pierson*, *supra* note 45 (describing how Apple shifted local user data onto China-based servers after the Chinese state-run media raised national security concerns about the iPhone's location-tracking feature).

[47] *Id.*

[48] 453 U.S. 280, 307 (1981).

> opting not to pay the price for increased and more efficient enforcement of criminal laws.[49]

Apple has a point. Though not one of the examples the Apple used, the tragedy of the Sandy Hook Elementary School shooting does illustrate "society opting not to pay the price" for greater security. In December 2015 an NBC News analysis found that in the three years since Adam Lanza killed twenty children and six adults at the Sandy Hook Elementary School, 555 children had been killed by intentional and unintentional gun violence.[50] As horrific as those numbers are, they pale in comparison with the 1,907 children killed as occupants of motor vehicles during approximately the same period.[51] The Center for Disease Control (CDC) estimates that in 2014 alone, 121,350 children age twelve and under suffered a vehicle-related injury.[52]

What is particularly disturbing is how easily avoidable so many of those deaths and injuries were. The Insurance Institute for Highway Safety and the Highway Loss Data Institute insist that "proper restraint use can reduce these fatalities."[53] They contend that studies show that the correct use of car seats can reduce these fatalities. "Restraining children in rear seats instead of front seats reduces fatal injury risk by about three quarters for children up to age 3, and almost half for children ages 4 to 8."[54]

For its part, the CDC says that in 2014, 34% of the children who were killed were "not buckled up."[55] The CDC also says that a study found that "more than 618,000 children ages 0 to 12 rode in vehicles without the use of a child safety seat or booster seat or a seat belt at least some of the time."[56] It "recommends car seat laws and car seat distribution plus education programs to increase restraint use and decrease injuries and deaths to child passengers."[57]

These statistics indicate that draconian enforcement of car seat laws

---

[49] Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 35, *In re* 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, No. ED 15-0451M (C.D. Cal. Feb. 25, 2016) [hereinafter Mot. to Vacate].

[50] Mike Brunker & Polly DeFrank, *Since Sandy Hook, an American Kid Has Died by a Gun Every Other Day*, NBC NEWS (Dec. 14, 2015, 5:01 AM), http://www.nbcnews.com/news/us-news/sandy-hook-american-kid-has-died-gun-every-other-day-n478746 [https://perma.cc/5CE7-B8QM].

[51] *Child Safety*, INS. INST. FOR HIGHWAY SAFETY & HIGHWAY LOSS DATA INST. (Nov. 2016), http://www.iihs.org/iihs/topics/t/child-safety/fatalityfacts/child-safety [https://perma.cc/5N47-2JWU].

[52] *Child Passenger Safety: Get the Facts*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/motorvehiclesafety/child_passenger_safety/cps-factsheet.html [https://perma.cc/N8YJ-T5RR] (last visited March 15, 2017).

[53] *Child Safety*, *supra* note 51.

[54] *Id*.

[55] *Child Passenger Safety: Get the Facts*, *supra* note 52.

[56] *Id*.

[57] *Id*. ("Prevention" tab).

would likely save more children than restrictions on guns. But even if Apple's suggestion that Americans are willing to "pay the price for increased and more efficient enforcement of criminal laws"[58] is correct, that is not necessarily the case here. Among other things, the Apple-FBI confrontation involved terrorism, something markedly different in the public's mind. For example, a September 2016 Monmouth University poll found that 56% of Americans believed that the government was not doing enough to prevent a future attack.[59]

The terrorism concern is understandable. In his new book, *Thank You for Being Late*, author Thomas Friedman makes the point that today's technology can create super-empowered terrorists, where even a single individual can wreak havoc on unprecedented numbers of people.[60] Even more clearly than the Monmouth University poll, a Quinnipiac University poll in September 2016 found that only 27% of Americans believed government's antiterrorism policies went "too far [in] restricting [the average person's] civil liberties," while 51% said those policies "have not gone far enough to adequately protect the country."[61] In short, encryption—with its potential as a tool of terrorism—poses a unique threat to public safety beyond that of ordinary criminality, which Apple seems to be referencing.

V. THE SOCIAL JUSTICE QUESTIONS

Law enforcement needs to comply with the Constitution and other legal requirements, and that typically requires getting a warrant or order from a court. When that happens, law enforcement ought to get the access the judge authorizes but no more. The Supreme Court in *Riley v. California* recognized the increased privacy concerns surrounding modern information technology—and specifically cell phones—and has extended the range of Fourth Amendment protection accorded to devices, but the Court has never suggested that the technologies ought to be beyond judicial process if a company can make the technology hyper secure.[62]

That said, no company should think itself above the law. Apple repeatedly cast the issue as one requiring resolution in the legislature. But in the interim, Apple seems to want the power to decide sensitive questions

---

[58] Mot. to Vacate, *supra* note 49, at 35.

[59] *2016 Brought Out Worst in People: Seven Percent Report Ending Friendship over Presidential Race*, MONMOUTH U. POLLING INST. (Sept. 28, 2016), https://www.monmouth.edu/polling-institute/reports/MonmouthPoll_US_092816/ [https://perma.cc/E5NU-7CDH].

[60] THOMAS L. FRIEDMAN, THANK YOU FOR BEING LATE: AN OPTIMIST'S GUIDE TO THRIVING IN THE AGE OF ACCELERATIONS 277, 279 (2016).

[61] *Clinton 44 – Trump 43, Too Close to Call, Quinnipiac University National Poll Finds; Democrat Has 9-Point Lead on Tonight's Debate*, QUINNIPIAC U. POLL (Sept. 26, 2016), https://poll.qu.edu/images/polling/us/us09262016_Up52mqb.pdf/ [https://perma.cc/7XB6-KBQ3].

[62] Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

of public security. Along these lines, former Director of the CIA John Brennan commented on the Apple-FBI case by observing that tech companies are now able to supplant the judgment of not just law enforcement, but of the courts as well.[63]

Therefore, if a judge issues a writ that says a safety deposit box in a bank must be opened up because there is something in there that is either inculpatory, exculpatory, or something that is going to allow us to prevent a crime, the bank owner has a legal obligation to open it up. The same situation happens with a warehouse owner, or somebody who owns an apartment building.

Now, private sector companies are getting the ability to say to the government, and to the courts: "[N]o, I'm going to determine what the government is going to be able to see or not."[64]

Put another way, should a company be allowed to refuse to open some kind of a safe, so as to allow a child pornographer to flaunt a bona fide search warrant? Should a certain class of criminals be permitted to avoid searches simply because they can afford to buy some kind of high-end safe or data encryption device? Why should people who, for example, send letters searchable with a warrant enjoy less privacy than someone who can afford the latest high-tech data gadget?

This reiterates the fallacy of Craig Federighi, Apple's Vice President, that "nothing is more important than the safety" of Apple customers; that logic does not comport with the fact that few things are more valuable to the most dangerous terrorists and criminals than the ability to conceal their communications from law enforcement and the courts.[65] If Apple (or anyone else) is allowed to sell devices that allow terrorists to plot and plan in secret, those terrorists will surely be customers, as will a host of other deviants and criminals.

Of course, the FBI and other law enforcement agencies still have to comply with the law, even though they now have a way into the phone at issue in the San Bernardino case. The ethical question is: given the horrific terrorist incident involved, was it ethical for a company to delay law enforcement's access to this particular phone where the owner of the phone wanted the FBI to have that access?

Some can literally afford to wait. After all, Silicon Valley is one of the wealthiest places on earth. The tech moguls who live there have little to worry about in terms of security for themselves and their families, as they can afford to buy as many layers of protection as they want. The rest of the citizenry, however, depend upon law enforcement agencies for protection, and their success in that effort can depend upon the ability to get

---

[63] BRENNAN, *supra* note 13.

[64] *Id.*

[65] Federighi, *supra* note 8.

information in compliance with court orders. Fortunately, another attack did not take place this time, but we all can imagine a different outcome in some future case. Should security really depend upon our ability to buy it privately as tech tycoons can?

Make no mistake about it, the residents of Silicon Valley and similarly privileged enclaves are concerned about their own security and are using their economic superiority to ensure it in ways that most Americans cannot. A recent *New Yorker* article addressing the "Doomsday Prep for the Super-Rich," pointed out that "[s]ome of the wealthiest people in America—in Silicon Valley, New York, and beyond—are getting ready for the crackup of civilization."[66] The article noted that:

> Survivalism, the practice of preparing for a crackup of civilization, tends to evoke a certain picture: the woodsman in the tinfoil hat, the hysteric with the hoard of beans, the religious doomsayer. But in recent years survivalism has expanded to more affluent quarters, taking root in Silicon Valley and New York City, among technology executives, hedge-fund managers, and others in their economic cohort.[67]

If one of Apple's motives for resisting the court order centered on its financial interests and brand value, perhaps Congress should devise a market-driven solution and create an appropriate cause of action for victims of terrorist incidents or other crimes. For example, if the evidence shows that the perpetrator had an encrypted device, a rebuttable presumption that such a device facilitated a plaintiff's victimization might be created by statute. The company could then choose to either provide access to the device to demonstrate that it had no connection with the incident, or accept the liability and inject that cost into the price of the device. Experience with big business—auto manufacturers, drug makers, chemical giants, tobacco companies, and more—shows that too often it needs to be motivated by the fear of lawsuits in order to take actions to protect public safety.

By obliging the FBI to turn to a private contractor to crack the encryption, Apple may have incentivized legitimate companies to get into the business of cracking phones and other high-tech devices for law enforcement. In essence, they have broadened the legal market for hackers and others.

Moreover—and rather ironically—Apple's intransigence may have backfired. As journalist Chris Smith observed, the success of the FBI's contractor "proves what we all suspected: that independent security companies and hackers know how to bypass the safety of the iPhone and

---

[66] Osnos, *supra* note 12.

[67] *Id*.

other devices if need be."[68] In essence, Apple created a legitimate market for hacking its phones on behalf of law enforcement. Moreover, instead of controlling the ability to unlock the phones, as would have been the case had Apple complied with the initial demand, that capability is now in the hands of the FBI—and it appears that the FBI is willing to share its success with other law enforcement agencies.[69]

Indeed, did Apple's recalcitrance endanger its own customers? Recall that Apple itself said that once an encryption-cracking protocol was developed, the technique could be used over and over again, on any number of devices. Apple said that "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."[70] It seems that tech companies are better off complying with court orders, and using or developing their own means of accessing their own products, than they are at acting in a way that invites other entities, over whom they have no control, to set up shop to serve law enforcement in these kinds of situations.

CONCLUSION

This brief Essay can at best be said to touch upon just a few of the issues raised by the "going dark" debate. That debate is hardly over. In August 2016, FBI Director James Comey described the situation of some 5,000 cell phones forwarded to the FBI for forensic examination. Comey said of the cell phones:

> About 650 of them we could not open. We did not have the technology. We can't open them. They are a brick to us. Those are cases unmade. That's evidence unfound. That has a significant impact on our work and on the work of law enforcement. We see this shadow, this inability to execute on court orders, becoming more and more a part of our life as encryption—especially strong encryption for data at rest, default encryption on devices—becomes a bigger feature of our life.[71]

---

[68] Chris Smith, *4 Reasons Why the FBI Unlocking the San Bernardino iPhone Without Apple Is Bad News*, BGR (Mar. 25, 2016, 7:45 AM), http://bgr.com/2016/03/25/apple-fbi-san-bernardino-iphone-hack/ [https://perma.cc/ET2Z-AN8K].

[69] Salvador Hernandez, *FBI Tells Local Law Enforcement It Will Help Unlock Phones*, BUZZFEED (Apr. 2, 2016, 12:22 AM), https://www.buzzfeed.com/salvadorhernandez/fbi-tells-local-law-enforcement-it-will-help-unlock-phones?utm_term=.rcazozRAX#.npMGJGxy9 [https://perma.cc/5ZR4-JW52].

[70] Cook, *supra* note 29.

[71] James B. Comey, Dir., Fed. Bureau of Investigation, Finding the Balance We Need in Law and Life, Address Before the American Bar Association Annual Meeting (Aug. 5, 2016),

Of course, in a real way, the "going dark" debate raises profound issues about the role of technology in our society. In a fascinating (albeit hyper partisan) essay considering the recent election, *Wired* Editor-at-Large Jason Tanz makes some interesting observations about the impact of communication technologies on contemporary political life, as well as somewhat indirect comments on the prescience and wisdom (or, more accurately, the absence of the same) of some tech entrepreneurs.[72]

Ruefully noting that President Trump used the "tools and language of the technocracy" to gain the White House, Tanz concludes that Silicon Valley efforts at designing technology to "maximize engagement . . . inadvertently created hives of bias-confirmation and tribalism."[73]

If one overlooks Tanz's politics, he does pose some trenchant broader questions that resonate in social justice. As he says, society needs to ask itself "bigger questions":

> Questions like: Is technology always an ennobling force? Questions like: Does allowing humanity untrammeled access to one another always result in a better world? Questions like: Are individuals capable of processing all the information that they once relied on institutions to process for them? Questions like: After people free themselves from their social and cultural shackles, then what?[74]

The full essay does suggest that Tanz has a sense of his own elitism, but the power of his questions remains. In a free society, to what extent should the byte barons of Silicon Valley determine what law enforcement professionals can and cannot do, particularly when they can insulate themselves from the consequences of their decisions?

Congress may act. In an election year when partisanship seems to know no limits, leaders from the two parties did work together to try to reign in the tech moguls. Senators Dianne Feinstein (D-Cal.) and Richard Burr (R-N.C.) authored a draft bill entitled the "Compliance with Court Orders Act of 2016."[75] Its key section simply said:

> To uphold both the rule of law and protect the interests and

---

https://www.fbi.gov/news/speeches/finding-the-balance-we-need-in-law-and-life [https://perma.cc/B42A-WGWE].

[72] *See* Jason Tanz, *How Silicon Valley Utopianism Brought You the Dystopian Trump Presidency*, WIRED (Jan. 20, 2017, 5:19 PM), https://www.wired.com/2017/01/silicon-valley-utopianism-brought-dystopian-trump-presidency [https://perma.cc/M2QH-QL9T].

[73] *Id*.

[74] *Id.*

[75] Compliance with Court Orders Act of 2016, 114th Cong. (Discussion Draft 2016), https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf [https://perma.cc/3N6P-YANZ]; Press Release, Office of Sen. Dianne Feinstein, Intelligence Committee Leaders Release Discussion Draft of Encryption Bill (Apr. 13, 2016) (on file with author).

> security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data . . . .[76]

The proposal immediately drew howls of protest from the tech industry, apoplectic over what they claimed—with some real logic—"basically outlaws end-to-end encryption."[77] The bill died.

Despite the poor reception for the Feinstein-Burr effort, Austin Carson, a legislative director for House Homeland Security Chairman Michael McCaul, said that McCaul will likely "re-introduce legislation to create a commission charged with examining tradeoffs between privacy and security in digital technology" in 2017.[78] Carson said that is far better than having events such as cases "where someone's child's been abducted . . . [or one] with national security implications" drive policy.[79] He is probably right when he predicted that if such events occur "it's going to be a horribly irrational conversation."[80]

Commissions and studies are all well and good, but there is little to suggest that there is a better way of finding that balance in much the same way it's always been—that is, for the courts to determine what is or is not permitted by the Constitution and the applicable statutes. There is nothing to dispute the idea that most people are satisfied with having the courts make these tough calls.

Of course, as a society, we can decide that we want more privacy than the Constitution or existing law might provide, but we ought not kid ourselves that there is no cost to doing so. It is certain that every terrorist, drug dealer, Wall Street cheat, sex-slaver, and crook of every variety will use a secure device if they think it will shield them from law enforcement, and to the extent that using such devices fulfills that desire, we have to expect and accept more terrorism and more crime. Significantly, that cost and risk will not be borne by those who are profiting from the devices, but by those without the resources or ability to protect themselves.

---

[76] Compliance with Court Orders Act of 2016, *supra* note 75.

[77] Andy Greenberg, *The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate*,*'* WIRED (Apr. 8, 2016, 11:16 AM), https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/ [https://perma.cc/W9HA-GXU3] (quoting Joseph Lorenzo Hall, chief technologist of the Center for Democracy and Technology).

[78] Joseph Marks, *Encryption Wars Will Return One Way or Another*, NEXTGOV (Jan. 23, 2017), http://www.nextgov.com/cybersecurity/2017/01/encryption-wars-will-return-one-way-or-another/134802/?oref=nextgov_today_nl [https://perma.cc/B34G-D4GK].

[79] *Id.*

[80] *Id*.