American University Law Review

Volume 66 | Issue 5 Article 4

2017

Holding the FBI Accountable for Hacking Apple's Software Under the Takings Clause

Mark S. Levy
American University Washington College of Law

Holding the FBI Accountable for Hacking Apple's Software Under the Takings Clause

Abstract

Smartphones have swiftly replaced most-if not all-conventional methods of sending, receiving, and storing personal information. Letters, address books, calendars, and trips to the bank have been rendered obsolete by tools such as text messaging, digital contacts, iCal, and mobile banking apps. Although these digital alternatives are convenient, they are not immune from attack. Therefore, to remain competitive, technology companies must maintain safe and secure platforms on which users may freely store and share their personal information.

Apple Inc., for example, strives to protect its users' intimate information, consequently earning a reputation for prioritizing security. Like a king protecting his castle, Apple has erected a variety of technological and legal barriers to guard its users' data and ward off unwanted intruders from vulnerabilities at a variety of stages. First, to protect user data from unauthorized access, Apple's software authorizes iPhone users to set their own passcode. Next, Apple encrypts its iPhone software, essentially placing adigital padlock on its software to preclude any software alterations, including the user-determined passcode functionality. Lastly, Apple copyrights its encryption padlock, discouraging rogue actors from circumventing its technology and security features in fear of civil or criminal implications.

In the spring of 2016, however, the federal government pillaged Apple's digital fortress, overcoming each of these barriers. The Federal Bureau of Investigation (FBI) was investigating the terrorist attack in San Bernardino, California, and Apple's security mechanisms precluded access to a shooter's iPhone, which was locked with the user-determined passcode. Nonetheless, the FBI hired professional hackers to alter Apple's software, thereby circumventing Apple's encryption and ignoring Apple's copyrights, to access the iPhone.

Although the FBI opened just this one phone, just this one time, its hacking has much broader implications. By altering Apple's software to circumvent its encryption, it smashed Apple's digital padlock, essentially creating a master key capable of opening hundreds of millions of iPhones, jeopardizing users' intimate information. The FBI has devalued Apple's coveted security and risked Apple's reputation. Despite Apple's copyright, Apple has no statutory remedy available; however, the Takings Clause in the Fifth Amendment of the United States Constitution affords Apple a simple solution.

This Note contributes to the contentious debate about prioritizing individual privacy in the face of increasingly innovative and complex national security threats. It suggests a novel way to deter governmental intrusion by establishing that Apple's copyrights are "prroperty" under the Fifth Amendment and by characterizing the FBI's investigative conduct in the San Bernardino case as a "taking" under the Fifth Amendment. Constitutionally requiring the federal government to pay 'just compensation" necessarily compels it to consider in its calculus the economic consequences of circumventing a technology company's encryption, potentially preventing such intrusion in the first place.

NOTE

HOLDING THE FBI ACCOUNTABLE FOR HACKING APPLE'S SOFTWARE UNDER THE TAKINGS CLAUSE

MARK S. LEVY*

Smartphones have swiftly replaced most—if not all—conventional methods of sending, receiving, and storing personal information. Letters, address books, calendars, and trips to the bank have been rendered obsolete by tools such as text messaging, digital contacts, iCal, and mobile banking apps. Although these digital alternatives are convenient, they are not immune from attack. Therefore, to remain competitive, technology companies must maintain safe and secure platforms on which users may freely store and share their personal information.

Apple Inc., for example, strives to protect its users' intimate information, consequently earning a reputation for prioritizing security. Like a king protecting his castle, Apple has erected a variety of technological and legal barriers to guard its users' data and ward off unwanted intruders from vulnerabilities at a variety of stages. First, to protect user data from unauthorized access, Apple's software authorizes iPhone users to set their own passcode. Next, Apple encrypts its iPhone software, essentially placing a digital padlock on its software to preclude any software alterations, including the user-determined passcode functionality. Lastly, Apple copyrights its

* Note & Comment Editor, *American University Law Review*, Volume 66; J.D. Candidate, May 2017, *American University Washington College of Law*; B.A. Psychology, *James Madison University*. I am inordinately grateful to Nancy Turner, for her thoughtful counsel throughout the development of this Note, and to Lisa Southerland, for her valuable contributions during the publication process. I also would like to thank the talented *American University Law Review* staff for its hard work and meticulous focus.

encryption padlock, discouraging rogue actors from circumventing its technology and security features in fear of civil or criminal implications.

In the spring of 2016, however, the federal government pillaged Apple's digital fortress, overcoming each of these barriers. The Federal Bureau of Investigation (FBI) was investigating the terrorist attack in San Bernardino, California, and Apple's security mechanisms precluded access to a shooter's iPhone, which was locked with the user-determined passcode. Nonetheless, the FBI hired professional hackers to alter Apple's software, thereby circumventing Apple's encryption and ignoring Apple's copyrights, to access the iPhone.

Although the FBI opened just this one phone, just this one time, its hacking has much broader implications. By altering Apple's software to circumvent its encryption, it smashed Apple's digital padlock, essentially creating a master key capable of opening hundreds of millions of iPhones, jeopardizing users' intimate information. The FBI has devalued Apple's coveted security and risked Apple's reputation. Despite Apple's copyright, Apple has no statutory remedy available; however, the Takings Clause in the Fifth Amendment of the United States Constitution affords Apple a simple solution.

This Note contributes to the contentious debate about prioritizing individual privacy in the face of increasingly innovative and complex national security threats. It suggests a novel way to deter governmental intrusion by establishing that Apple's copyrights are "property" under the Fifth Amendment and by characterizing the FBI's investigative conduct in the San Bernardino case as a "taking" under the Fifth Amendment. Constitutionally requiring the federal government to pay "just compensation" necessarily compels it to consider in its calculus the economic consequences of circumventing a technology company's encryption, potentially preventing such intrusion in the first place.

TABLE OF CONTENTS

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge."

—Bruce Schneier[1]

INTRODUCTION

Employers customarily host workplace holiday parties to thank their employees and celebrate their hard work over the past year; nothing was customary, however, about one holiday party on December 2, 2015, in San Bernardino, California. The sounds of festive music and laughter were quickly replaced by deafening gunshots and screams for help when Syed Rizwan Farook and Tashfeen Malik opened fire on a crowd of innocent victims.[2] Fourteen people were violently slain; twenty-two people were senselessly injured.[3] The tragedy stirred emotions across the country, but it also relaunched an important legal debate about individual privacy.

Law enforcement officers often struggle to understand why individuals commit such heinous crimes, but these two assassins left behind one item that could provide clarity: an iPhone. However, the federal government encountered a roadblock in its investigation when it sought to access the locked iPhone of one of the shooters.[4] The Federal Bureau of Investigation (FBI) hoped to find inculpatory evidence and uncover other parties who may have been involved in the attack.[5] But, a user-determined passcode blocked law enforcement's access to the phone, and the FBI risked the phone's data automatically erasing if it guessed the wrong passcode just ten

---

1. DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 238 (2015).

2. Nathan Rott, *San Bernardino Shooting's Signs Have Faded, but Memories Remain Piercing*, NPR (Dec. 2, 2016, 4:47 AM), http://www.npr.org/2016/12/02/504025469/san-bernardino-shootings-signs-have-faded-but-memories-remain-piercing.

3. *Id.*

4. *See generally* Steven Musil, *Apple Ordered to Help Unlock San Bernardino Shooter's iPhone*, CNET (Feb. 16, 2016, 6:00 PM), https://www.cnet.com/news/apple-ordered-to-unlock-san-bernardino-shooters-iphone.

5. Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300 at 2, No. ED 15-0451M, 2016 WL 680288, at *2 (C.D. Cal. Feb. 16, 2016) [hereinafter Government's Ex Parte Application].

times.[6] Though it obtained a federal court order directing Apple Inc. ("Apple") to design new software that would help the agency open the iPhone,[7] the FBI felt the wheels of justice were turning too slowly, so it took matters into its own hands. It hired professional hackers to circumvent the shooter's passcode, smashing the digital lock that protected Apple's copyrighted software and jeopardizing the security and privacy of hundreds of millions of people storing sensitive information on their iPhones.[8]

The events following the San Bernardino massacre stoked the coals of a fire already burning bright among individuals with varying religions, philosophies, and ideologies. They reinvigorated a debate the nation has wrestled with many times since September 11—one concentrated at the intersection of national security and individual privacy. Americans differ as to how the federal government should balance these competing interests,[9] but the debate does not always consider other important concerns, such as the extraordinary economic cost of exposing intimate information.

In the modern world, effortless access to information is within an arm's length at all hours of the day. We use devices like iPhones both to explore the depths of the Internet and to store our most intimate personal information. Although information is the lifeblood of our economy and we often desire open access, we also go to great lengths to protect it.[10] Apple has done so by encrypting users' personal

---

6. *FBI Overpaid $999,900 to Crack San Bernardino iPhone 5c Password*, REGISTER (Sept. 19, 2016, 4:58 AM), http://www.theregister.co.uk/2016/09/19/fbi_overpaid_999900_to_crack_san_bernardino_iphone_5c_password.

7. *See* Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html (describing the FBI's troubles opening the iPhone and its plea to the court that "Apple had the 'exclusive' means to bypass the security features on the phone").

8. Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. 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.

9. *See* Lee Rainie & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR.: FACT TANK (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns (estimating that as of December 2015, "56% of Americans were more concerned that the government's anti-terror policies have not gone far enough to protect the country, compared with 28% who expressed concern that the policies have gone too far in restricting the average person's civil liberties").

10. *See, e.g.*, Nate Lord, *What Is Data Encryption?*, DIGITAL GUARDIAN (Jan. 27, 2017), https://digitalguardian.com/blog/what-data-encryption (detailing that

information stored in iPhones—essentially, a lock with only one irreproducible key. However, these user-determined passcodes erect formidable barriers for law enforcement officials investigating crimes. Officials have recently begun developing ways to circumvent this technology, but developing such access is not cheap, and it is the technology company—not the government—that bears the ultimate cost. While investigating the San Bernardino shooters, the federal government crafted a master key capable of opening any user-determined lock, jeopardizing the privacy of our personal information and thus harming Apple's security and reputation.

This type of clandestine security breach casts a wide shadow, leaving many of us in the dark about the government's attempt at balancing national security and individual privacy. Users store a variety of intimate information on their iPhones: financial records, emails, text messages, family photos, and personal notes. Because the software to circumvent Apple's user-determined passcodes did not exist before, the FBI altered Apple's copyrighted software.[11] The alteration empowered the FBI to access not only the San Bernardino shooter's iPhone but also any iPhone 5c running the same operating system.[12] The prospect that a similar alteration may also empower the FBI to access *any* iPhone running *any* operating system should alarm the millions of users who rely on Apple's strong reputation for data security.

The U.S. Constitution, however, provides an explicit remedy for such governmental intrusions. The Takings Clause of the Fifth Amendment prohibits the federal government from taking "private property . . . without just compensation."[13] The Framers "designed [it] to bar Government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole."[14] However, Apple alone shouldered the public's burden amid the investigation into the shooters in San Bernardino.

This Note advocates that the federal government owes Apple "just compensation" under the Takings Clause of the Fifth Amendment for hacking Apple's copyrighted software. Part I canvases the Takings Clause and specifically discusses which items constitute "property" under the Fifth Amendment and which forms of governmental intrusion constitute a "taking" under the Fifth Amendment. Next, Part II outlines

---

"[d]ata encryption translates data into . . . code, so that only people with access to a secret key (formally called a decryption key) or password can read it").

11. Nakashima, *supra* note 8.

12. *Id.*

13. U.S. CONST. amend. V.

14. Armstrong v. United States, 364 U.S. 40, 49 (1960).

the federal government's role during the San Bernardino investigation, describing the legal battle between Apple and the FBI and the FBI's forcible breach into Apple's software. Part III provides the necessary background on copyrights and contends that (1) copyrights constitute "property" under the Fifth Amendment, and (2) the FBI's iPhone hacking constitutes a "taking" under the Fifth Amendment. Consequently, this Note concludes that the federal government owes Apple "just compensation" under the Takings Clause because the FBI "took" Apple's property by designing and distributing software that circumvented Apple's copyrighted iPhone software.

I. TAKINGS CLAUSE OF THE FIFTH AMENDMENT

Perhaps the most important value of law in society is the right it confers on an individual to exclude others from his or her property.[15] As a corollary, the right to exclude also includes the right to consume, transfigure, transfer, bequeath, pledge as collateral, or otherwise dispose of property as the owner wishes.[16] The Founding Fathers considered the right to exclude one of the pillars buttressing our Republic, defining "property broadly to include 'Life, Liberty and Estate.'"[17] Whether a property right is based in common law, such as real and personal property, or in statute, such as patents and copyrights, its economic value is in the owner's right to the sole enjoyment of any benefits accruing from the property.

Legal scholars have described property ownership as a "major battleground" to resolve the conflict stemming from "individual liberty and privacy on the one hand and community and equality on the other."[18] The Supreme Court has agreed, characterizing "the right to exclude others" as "one of the most essential sticks in the bundle of rights that are commonly characterized as property."[19] But,

---

15. In fact, the motivation behind the initial exploration of the Americas was to "exploit the economic opportunities" that lay dormant in the undeveloped landscape of the Western hemisphere. Kenneth L. Sokoloff & Stanley L. Engerman, *Institutions, Factor Endowments, and Paths of Development in the New World*, 14 J. ECON. PERSP. 217, 220 (2000).

16. Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998).

17. Stuart Bruchey, *The Impact of Concern for the Security of Property Rights on the Legal System of the Early American Republic*, 1980 WIS. L. REV. 1135, 1136–37 (quoting JOHN LOCKE, *Second Treatise of Government*, *in* TWO TREATISES OF GOVERNMENT 341 (Peter Laslett ed., 1964) (1690)) (opining that "the most important value of the Founding Fathers of the American constitutional period was their belief in the necessity of securing property rights").

18. Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1345 (1993).

19. Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979).

this fundamental right to exclude is not perfect. However natural these rights may seem, or however entitled to them we may feel, property rights are arbitrary and meaningless without "some institutional structure that stands ready to enforce these rights."[20] Ironically, however, the "institutional structure" charged with protecting these rights also reserves for itself the authority to undermine any legally obtained interest in property.[21]

Though the Framers reserved the federal government's ability to appropriate private property for public use, they did so with the caveat that a displaced owner must be compensated for the taking. In the eighteenth century, the Framers imported the principle of eminent domain from the Magna Carta, incorporating it into their young colonial governments and eventually the Fifth Amendment of the United States Constitution.[22] The Takings Clause in the Fifth Amendment provides that the federal government shall not take "private property . . . for public use, without just compensation."[23] The Framers sought to prevent the "Government from forcing some people alone to bear public burdens" and to protect expectations of exclusivity deriving from property.[24] It appears the Framers specifically feared that private citizens would be deprived of their property, subjected to intrusive government interference, or denied the opportunity to use property to their competitive advantage.

The Supreme Court's jurisprudence interpreting the Takings Clause evinces a clear understanding that the federal government must pay for private property that it chooses to appropriate. Any comprehensive analysis includes two critical inquiries: (1) whether the item at issue constitutes "property" under the Fifth Amendment,

---

20. Merrill, *supra* note 16, at 733.

21. *See* Steven J. Eagle, *Just Compensation for Permanent Takings of Temporal Interests*, 10 FED. CIR. B.J. 485, 486 (2001) (acknowledging that the Takings Clause "implicitly recognizes that eminent domain is an inherent attribute of both the national and state governments").

22. Indeed, the Magna Carta proscribed the King from appropriating "corn or other provisions from any one [sic] without immediately tendering money therefor." Horne v. Dep't of Agric., 135 S. Ct. 2419, 2426 (2015) (quoting MAGNA CARTA cl. 28 (1215), *in* WILLIAM SHARP MCKECHNIE, MAGNA CARTA: A COMMENTARY ON THE GREAT CHARTER OF KING JOHN 329 (2d ed. 1914)). John Locke, a colonist of Carolina, prescribed "just compensation" for government takings in the 1669 Fundamental Constitution of Carolina. *See* Andrew S. Gold, *Regulatory Takings and Original Intent: The Direct, Physical Takings Thesis "Goes Too Far"*, 49 AM. U. L. REV. 181, 209 (1999) (citing Fundamental Constitutions of Carolina art. 44 (1669), *reprinted in* 1 BERNARD SCHWARTZ, THE BILL OF RIGHTS: A DOCUMENTARY HISTORY 8, 115 (1971)).

23. U.S. CONST. amend. V.

24. Armstrong v. United States, 364 U.S. 40, 49 (1960).

and (2) whether the government's conduct with the item constitutes a "taking" under the Fifth Amendment.[25]

A. Identifying What Constitutes "Property"

Despite the Framers' concerns about protecting property rights, the Takings Clause fails to define "property." The Supreme Court, however, has defined an expansive range of property that, if taken, warrants compensation. For instance, the Court has deemed the following "property" under the context of the Fifth Amendment: realty, including buildings,[26] easements,[27] and the corresponding airspace above the property;[28] personalty[29] and liens on personalty;[30] government seizure of a business;[31] and intellectual property, such as patents,[32] trade secrets,[33] and rights under a valid contract.[34] Thus, the Court considers "property" under the Takings Clause to include most recognized property rights—whether derived from the Constitution, statutes, or common law—that confer exclusivity on the owner.

---

25. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1000 (1984); *see also* Note, *Copyright Reform and the Takings Clause*, 128 HARV. L. REV. 973, 975–78 (2015).

26. *See, e.g.*, Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1007, 1019 (1992) (addressing a South Carolina law that prohibited a property owner from erecting a house on beachfront property); Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 421 (1982) (discussing a New York law requiring landlords to permit a cable television company to install equipment on the building).

27. *See, e.g.*, United States v. Welch, 217 U.S. 333, 339 (1910) (finding that "the discontinuance of" an easement, here a private right of way, constituted interference with a property right).

28. *See, e.g.*, United States v. Causby, 328 U.S. 256, 258, 266 (1946) (involving a dispute in which frequent military aircrafts flew within "the immediate reaches above the land").

29. *See, e.g.*, Horne v. Dep't of Agric., 135 S. Ct. 2419, 2424–25 (2015) (reviewing a federal statute obligating raisin growers to give a percentage of their crops to the government).

30. *See, e.g.*, Armstrong v. United States, 364 U.S. 40, 46 (1960) (assessing a dispute in which the government compelled petitioner to transfer valid liens against both hulls and material held for use in building boats).

31. *See, e.g.*, United States v. Pewee Coal Co., 341 U.S. 114, 115, 117 (1951) (considering a coal mine "possessed and operated for public use").

32. *See* James v. Campbell, 104 U.S. 356, 358 (1882) (explaining that a patent confers an "exclusive property in the patented invention which cannot be appropriated or used by the government itself, without just compensation, any more than it can appropriate or use without compensation land which has been patented to a private purchaser").

33. *See, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 990, 1003–04 (1984) (evaluating the EPA's obligating pesticide companies to disclose data that the agency later used to evaluate other pesticides).

34. *See* Lynch v. United States, 292 U.S. 571, 579 (1934) (concerning insurance policies under the War Risk Insurance Act of 1917).

Nonetheless, not all legal entitlements of exclusivity necessarily amount to "property" under the Fifth Amendment.[35] For instance, although copyrights confer the owner exclusivity to creative works such as literary and musical compositions,[36] the Court has remained silent on whether copyrights constitute "property" under the Fifth Amendment. However, various federal courts of appeals—including the First,[37] Second,[38] Fifth,[39] Sixth,[40] and Ninth[41] circuits—have suggested that governments may be obligated to compensate private individuals for taking, or even shortening the lives of, copyrights.[42] Legal scholars have also contended that the Takings Clause should apply to valid copyrights.[43] Realty and personalty certainly constitute "property" under

---

35. *Copyright Reform and the Takings Clause*, *supra* note 25, at 977 ("[T]he mere fact that a person enjoys some legal benefit does not entitle the person to continue enjoying it.").

36. U.S. COPYRIGHT OFFICE, CIRCULAR 1: COPYRIGHT BASICS 1 (2012), https://www.copyright.gov/circs/circ01.pdf.

37. *See* Lane v. First Nat'l Bank of Bos., 871 F.2d 166, 174 (1st Cir. 1989) (noting that copyrights are property, and if the state government "afford[ed] [the plaintiff] no just compensation for the wrongful confiscation of her property, the Takings Clause of the federal Constitution might at that point enable her to pursue a damage remedy in federal court").

38. *See* CCC Info. Servs., Inc. v. Maclean Hunter Mkt. Reports, Inc., 44 F.3d 61, 74 (2d Cir. 1994) (cautioning, in dicta, that "a state legislature or administrative body depriv[ing] the copyright owner of its property would raise very substantial problems under the Takings Clause of the Constitution").

39. *See* Chavez v. Arte Publico Press, 157 F.3d 282, 288 (5th Cir. 1998), *reh'g en banc granted, vacated*, 178 F.3d 281 (5th Cir. 1998), *and on reh'g en banc*, 180 F.3d 674 (5th Cir. 1999) ("[C]opyrights constitute intangible property that, for some purposes at least, receives constitutional protection.").

40. *See* Cawley v. Swearer, No. 90-1981, 1991 WL 108725, at *3 (6th Cir. June 20, 1991) (per curiam) (stating that "the Copyright Act does not preempt the Fifth Amendment's Takings Clause").

41. *See* Practice Mgmt. Info. Corp. v. Am. Med. Ass'n, 121 F.3d 516, 520 (9th Cir. 1997), *amended*, 133 F.3d 1140 (9th Cir. 1998) (affirming that the plaintiff's copyright "should be enforced" despite the copyrighted material being adopted by federal regulation—in part because the regulatory adoption would otherwise create Takings Clause concerns).

42. At least one appeals court, the Federal Circuit, has acknowledged but so far avoided the question. *See* Zoltek Corp. v. United States, 672 F.3d 1309, 1327 (Fed. Cir. 2012) (per curiam), *vacated*, 672 F.3d 1309 (Fed. Cir. 2012) (electing not to "reach the issue of the Government's possible liability under the Constitution for a taking").

43. *Compare Copyright Reform and the Takings Clause*, *supra* note 25, at 981–82 (arguing that "the weight of scholarly opinion is that copyrights are property for takings purposes"), *and* Thomas F. Cotter, *Do Federal Uses of Intellectual Property Implicate the Fifth Amendment?*, 50 FLA. L. REV. 529, 532 (1998) (noting that the issue of copyrights and takings "has evoked wildly differing responses, ranging from the view that virtually

the Fifth Amendment, yet there is no legally binding Supreme Court precedent on whether the government owes a private individual "just compensation" for appropriating a copyright.

B. Identifying What Constitutes a "Taking"

Although the "property" at issue may satisfy the first inquiry under the Fifth Amendment, the government's conduct must also satisfy the second inquiry for protection: whether the conduct amounts to a "taking." Conventional notions of what constitutes a taking involve physical deprivation of land, such as when the government acquires a parcel of private land for an easement or destroys an automobile in the process of extinguishing a fire in an adjacent building.[44] However, the Court has also labeled unconventional deprivations of private property as takings.[45] For instance, if the effects of a governmental regulation are so severe as to essentially "deprive the owner of all or most of his interest" in the property, courts may accurately characterize the conduct as a taking.[46]

The legal community may prefer hard and fast rules, but the checkered jurisprudence concerning the Takings Clause has evinced anything but clarity. The Court has "recognized few invariable rules" and "has generally eschewed" any rigid "magic formula" to compute a government taking.[47] Rather, takings analyses can be more aptly depicted as a spectrum of governmental interference, varying in the magnitude of deprivation.[48] At one end of the spectrum, conduct

---

all government uses of intellectual property constitute takings to the view that virtually none of them do"), *with* Tom W. Bell, *Copyright as Intellectual ~~Property~~ Privilege*, 58 SYRACUSE L. REV. 523, 545–46 (2008) (advocating that copyrights are "intellectual privilege[s]" rather than property interests under the Takings Clause).

44. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1004 (1984) (characterizing traditional deprivations of property under the Takings Clause as "governmental acquisition[s] or destruction of . . . property").

45. *See* United States v. Gen. Motors Corp., 323 U.S. 373, 378 (1945) ("Governmental action short of acquisition of title or occupancy has been held, if its effects are so complete as to deprive the owner of all or most of his interest in the subject matter, to amount to a taking.").

46. *See id.* For instance, a city ordinance that bars land owners from constructing buildings on their property, rendering them valueless, may properly constitute a governmental taking. *See* Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1007, 1030 (1992).

47. Horne v. Dep't of Agric., 135 S. Ct. 2419, 2437 (2015) (Sotomayor, J., dissenting) (quoting Ark. Game & Fish Comm'n v. United States, 568 U.S. 23, 31 (2012)); *see also Lucas*, 505 U.S. at 1015.

48. In *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003 (1992), the Court identified "two discrete categories of regulatory [takings]": (1) "regulations that compel the property owner to suffer a physical 'invasion' of his property," and (2)

fails to rise to the level of a "taking" where it clearly constitutes a governmental nuisance rather than a governmental deprivation.

At the other end of the spectrum, conduct clearly constitutes a "taking" where the government undoubtedly deprives the owner of complete use of the property, such as capturing land and deeming it a public easement.[49] The Court has branded this type of government conduct a "per se taking," of which there are two core varieties.[50] The first type of per se taking involves government conduct that either denotes or sanctions "permanent physical occupation" of property regardless of the public interest it serves. In *Loretto v. Teleprompter Manhattan CATV Corp.*,[51] for example, a statute required landlords to permit cable television companies to install their equipment on the roof of the building for the benefit of the tenants.[52] The Court found that the equipment installation amounted to a "permanent physical occupation" of the landlord's property, thereby constituting a taking.[53] The second type of per se taking involves government conduct that does not physically invade private property but nevertheless renders property economically worthless. For instance, in *Lucas v. South Carolina Coastal Council*,[54] a state statute prevented beachfront property owners from erecting any buildings on such property.[55] The Court found that these statutes constituted a taking because they rendered the lots "valueless" by "prohibit[ing] all economically beneficial use of [the] land."[56] In other words, the government "denie[d] an owner economically viable use of his land" vis-à-vis regulation.[57] Accordingly, per se takings are ostensibly

---

regulations that fall short of physical invasion, but deny "all economically beneficial or productive use of land." *Id.* at 1015; *see also* Bethany Berger, *The Illusion of Fiscal Illusion in Regulatory Takings*, 66 AM. U. L. REV. 1, 2–7 (2017) (exploring the takings spectrum); *Copyright Reform and the Takings Clause*, *supra* note 25, at 977–78 (bifurcating the discussion into distinct "modes of analysis": (1) "per se takings" and (2) "*Penn Central*" takings).

49. *See, e.g.*, United States v. Welch, 217 U.S. 333, 338–39 (1910) (deeming the government flooding of a private right of way to be a "taking").

50. *See, e.g.*, *Horne*, 135 S. Ct. at 2424–26, 2430 (finding a per se taking where the U.S. Department of Agriculture's Raisin Administrative Committee required raisin growers to give the government a portion of their raisin crops).

51. 458 U.S. 419 (1982).

52. *Id.* at 423.

53. *Id.* at 426.

54. 505 U.S. 1003 (1992).

55. *Id.* at 1007.

56. *Id.* at 1007, 1029.

57. *Id.* at 1016 (emphasis omitted). In *Lingle v. Chevron U.S.A. Inc.*, 554 U.S. 528 (2005), the Court lamented that whether a regulation "substantially advances" a

categorical and collectively possess attributes of aggressive encroachment on private property.

In between the two clear extremes of the governmental interference spectrum, "*Penn Central*" takings occupy the muddled middle ground in which courts analyze the totality of the circumstances to determine whether government conduct constitutes a taking.[58] Unlike per se takings, which prevent owners from enjoying *all* economic benefit from the property at issue, a "*Penn Central*" taking prevents owners from enjoying some *portion* of economic benefit from the property. In *Penn Central Transportation Co. v. New York City*,[59] New York City imposed "restrictions on the development of individual historic landmarks" and established a gatekeeper with the authority to approve or reject "any proposal to alter the exterior architectural features of [a] landmark."[60] Although the owner of such a historic landmark still had the ability to use and profit from the building, the ordinance deprived him of unfettered control of his property. A subsequently rejected proposal sparked litigation, but it also triggered a notable transformation in the law, prompting the Court to furnish three factors to determine whether governmental interference is tantamount to a constitutional taking requiring just compensation: (1) "the economic impact of the regulation on the claimant," (2) "the extent to which the regulation has interfered with distinct investment-backed expectations," and (3) "the character of the governmental action."[61] Essentially, in *Penn Central* takings, the government may justify the deprivation if it "substantially advance[s] legitimate state interests."[62] As a result, *Penn Central* takings require "situation-specific factual inquiries,"[63] and the outcome of challenges to governmental interference under the *Penn Central* takings theory is more fortuitous than challenges pursuant to the per se takings theory. *Penn Central* takings are a "relatively recent development" that arguably complicate an already murky area of law.[64]

---

legitimate government interest "is not a valid takings test," thus obviating the need for any analysis on the intent or purpose behind the government's conduct. *Id.* at 548.

58. *Copyright Reform and the Takings Clause*, *supra* note 25, at 1015.

59. 438 U.S. 104 (1978).

60. *Id.* at 107, 112.

61. *Id.* at 124; *see also* Kenneth J. Sanney, *Balancing the Friction: How a Constitutional Challenge to Copyright Law Could Realign the Takings Clause of the Fifth Amendment*, 15 COLUM. SCI. & TECH. L. REV. 323, 336 n.35 (2014).

62. *Lingle*, 544 U.S. at 540.

63. Ark. Game & Fish Comm'n v. United States, 568 U.S. 23, 32 (2012).

64. Sanney, *supra* note 61, at 333–35 (asserting that the approach has "created an unsettled and unpredictable body of law").

II. FBI'S JOURNEY TO HACK APPLE'S IOS SOFTWARE

The intrusive hacking into the Apple iPhone provides a sobering presentation of the federal government's power. The public widely condemned the malevolent terrorism that occurred in San Bernardino on December 2, 2015; however, the subsequent events that transpired in the U.S. District Court for the Central District of California incited a national conversation concerning the balance between individual privacy and national security. As the FBI scrambled to make sense of an otherwise senseless crime, it sought answers in the shooter's locked iPhone.[65] From the iPhone, the FBI sought to unlock the iPhone "to determine . . . who [the shooters] may have communicated with to plan and carry out the . . . shootings, where [the shooters] may have traveled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement."[66] To gain access to the iPhone, the FBI turned to a federal court, requesting that Apple unlock the iPhone to help the FBI make sense of what had happened.[67]

On February 16, 2016, roughly two months after the deadly shooting, the federal government filed an ex parte application for an order compelling Apple to assist the FBI in unlocking the iPhone.[68] The government pleaded with the court that, under the All Writs Act,[69] "Apple ha[d] the exclusive technical means" to unlock the iPhone and "Apple's assistance [was] necessary to effectuate the [valid search] warrant."[70] It claimed Apple's assistance was necessary because Apple designed its iOS 9 operating system to encrypt and protect the files stored on its devices.[71] Specifically, three technological barriers prevented the government from accessing the iPhone: (1) the phone

---

65. *See* Musil, *supra* note 4 (explaining that the iPhone of the San Bernardino shooter was "password protected, and investigators worr[ied] that the handset's encryption [would] erase its data after too many unsuccessful attempts to unlock the device").

66. Government's Ex Parte Application, *supra* note 5, at 2.

67. *Id.* at 1.

68. *Id.*

69. 28 U.S.C. § 1651(a) (2012) ("[A]ll [federal] courts . . . may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."). Although the government's utilization of the All Writs Act to compel Apple's cooperation generated controversy in and of itself, that topic is beyond the scope of this Note. *See* Amy Davidson, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, NEW YORKER (Feb. 19, 2016), http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

70. Government's Ex Parte Application, *supra* note 5, at 1, 16.

71. *Id.* at 5.

was "secured with a user-determined, numeric passcode"; (2) the phone had an "auto-erase function," which permanently destroyed its data "after 10 erroneous attempts at the passcode"; and (3) the encryption key was "fused into the phone itself during manufacture," so that Apple must "modify [the] software" to guarantee that the "auto-erase function is turned off" to protect the files.[72]

Despite a swift and succinct order granting the government's request and compelling Apple to assist in the investigation,[73] Apple moved to vacate the order shortly thereafter, proffering three essential reasons for its non-compliance.[74] First, Apple informed the court that iPhone users store intimate and vital information that would become "vulnerable to hackers, identity thieves, hostile foreign agents, and unwarranted government surveillance."[75] Apple characterized the government's efforts as crippling an otherwise secure product.[76] Second, Apple alerted the court that the software the government envisioned would effectively create a "back door" to its operating system, and that Apple would have to dedicate six to ten Apple engineers to "create a new version of the iPhone operating system designed to defeat [its] critical security features."[77] Essentially, the government wanted to create a "master key, capable of opening hundreds of millions of locks."[78] Third, Apple cautioned the court that other law enforcement operations—local, state, national, and international investigators wishing to unlock iPhone devices—would

72. *Id.* at 3–5.

73. *See* Order Compelling Apple, Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016) (ordering that Apple (1) "bypass or disable the auto-erase function," (2) "enable the FBI to submit passcodes to the SUBJECT DEVICE," and (3) "ensure that when the FBI submits passcodes to the SUBJECT DEVICE, software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware").

74. *See generally* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, *In re Search of an Apple iPhone*, No. ED CM 16-10 (SP) (C.D. Cal. Feb. 25, 2016) [hereinafter Apple's Motion to Vacate].

75. *Id.* at 1 (explaining that users store a wide variety of information on their phones, including "financial records and credit card information, health information, location data, calendars, personal and political beliefs, family photographs, [and] information about their children").

76. *See id.* at 2 (characterizing the government's position as wanting "Apple to create a crippled and insecure product"). Apple was also apprehensive about the forcible nature of the request, "like compelling a pharmaceutical company against its will to produce drugs needed to carry out a lethal injection." *Id.* at 26.

77. *Id.* at 2, 12–13.

78. *Id.* at 3.

also want the technology, warning that widespread access would destabilize its security system.[79] Accordingly, Apple argued—with the support of numerous tech giants that filed amicus briefs[80]—that the potential costs to millions of individuals relying on the security of the iPhone enormously outweighed the FBI's interest in investigating the case at issue.[81]

Before resolution of Apple's motion, however, the FBI unlocked the iPhone without Apple's assistance.[82] The FBI hired professional hackers to exploit a flaw in Apple's encryption software and develop hardware that could decipher the four-digit passcode without risking a data wipe from too many incorrect attempts.[83] Not only did the FBI side-step Apple to break into the iPhone, but the FBI has refused to release information on whom it hired and has classified the hackers' methodology, leaving the public with many unanswered questions.[84]

---

79. *Id.* at 3, 24 (counseling the court that "[o]nce the floodgates open, they cannot be closed"). For instance, Apple worried that acquiescence here would create precedent to force Apple inevitably to "turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user." *Id.* at 4.

80. *See, e.g.*, Brief for Lavabit LLC as Amicus Curiae Supporting Apple Inc.'s Motion to Vacate at 11, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Mar. 4, 2016) [hereinafter Lavabit Brief] (arguing that government acquiescence would "harm both [Apple's] competitive advantage, its reputation as a manufacturer of secure devices, and, by extension, harm other companies . . . that have developed secure storage methods"); Brief of AT&T Mobility LLC as Amicus Curiae Supporting Apple Inc. at 5, *In re Search of an Apple iPhone*, No. ED 15-0451M (C.D. Cal. Mar. 3, 2016) (claiming that "the government[] . . . risk[s] substantial harm to the security of millions of iPhones").

81. Moreover, Apple initially cooperated with the FBI, "devot[ing] substantial resources on a 24/7 basis to support the government's investigation," but the FBI mistakenly foreclosed the only opportunity in which Apple could have helped without creating a backdoor. *See* Apple's Motion to Vacate, *supra* note 74, at 10–11 (explaining that the FBI changed the iCloud password associated with the account, thus preventing the device from backing up its data automatically).

82. *See* Government's Status Report at 1–2, *In re Search of an Apple iPhone*, No. ED 15-0451M (C.D. Cal. Mar. 28, 2016) ("The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple . . . .").

83. *See* Nakashima, *supra* note 8.

84. Eric Tucker, *FBI Releases Documents Related to San Bernardino iPhone*, ASSOCIATED PRESS (Jan. 7, 2017), http://bigstory.ap.org/article/016259a14b8d4c3eb be784f6c564151f/fbi-releases-documents-related-san-bernardino-iphone (reporting that the FBI "released 100 pages of heavily censored documents related to its agreement with an unidentified vendor . . . but it did not identify whom it paid to perform the work or how much it cost"); *see also* Plaintiff's Cross-Motion for Summary Judgment at 5–8, Associated Press v. Dep't of Justice, No. 1:16-cv-01850-TSC (D.D.C.

III. WHY THE FBI OWES APPLE "JUST COMPENSATION"

Apple is the creator of the iPhone, a mini computer that can fit comfortably in your pocket and simultaneously process calls, text messages, emails, music, and more. The iPhone is one of the most innovative pieces of technology: *Fortune Magazine* reported on a poll that ranked the iPhone as the eighth greatest invention, one place below penicillin and six places above the refrigerator.[85] It is obvious, then, why Apple copyrighted its iPhone software and equipped it with a digital padlock.[86] Nonetheless, the federal government smashed that padlock, digitally trespassing and infringing on Apple's copyrighted software.[87]

Apple's encryption provided "Apple with the strongest means available to ensure the safety and privacy of its customers";[88] however, the government misappropriated that technology, thereby harming Apple's competitive advantage and depriving Apple of its intellectual property in violation of the Fifth Amendment.[89] Consequently, the federal government owes Apple "just compensation" for damaging Apple's product and reputation.

A. Circumventing Copyrighted Software

Traditionally, property has denoted something tangible, such as a tractor or even the land on which that tractor stood; however, intangible property also serves an important—if not more important—function in society. Just as a deed grants an individual the exclusive right to land, permitting him the sole right to maintain, neglect, sell, or bequeath it as he chooses, a copyright similarly grants an individual, usually the creator or author, the exclusive right to "original works of authorship," permitting him the sole right to reproduce, recreate, or distribute it as he chooses.[90] The purpose of

---

Feb. 20, 2017) (exemplifying litigation following the FBI's denial of Freedom of Information Act requests for records that would reveal the identity of the hackers and how much the FBI paid them).

85. Philip Elmer-DeWitt, *Brits Vote iPhone 8th Greatest Invention*, FORTUNE (May 20, 2010), http://fortune.com/2010/05/20/brits-vote-iphone-8th-greatest-invention.

86. *See infra* notes 90–92 and accompanying text (explaining the purpose of copyrights).

87. *See supra* Part II (discussing the FBI's conduct pertaining to Apple).

88. Apple's Motion to Vacate, *supra* note 74, at 5.

89. *See infra* Section III.B.2.

90. *See* 17 U.S.C. §§ 102, 106 (2012). Copyrights may include the following: "(1) literary works; (2) musical works, including any accompanying words; (3) dramatic works, including any accompanying music; (4) pantomimes and choreographic

copyrights is to encourage and "stimulate artistic creativity for the general public good" by granting the author a statutory monopoly on the fruits of his labor.[91] This exclusive "right to market" incentivizes authors to produce a work for the benefit of society because they know they will be the beneficiaries of any such efforts.[92]

Thus, when others invade an owner's valid copyright, the owner may enforce his right to exclude. In addition to prohibiting the simple reproduction of copyrighted work,[93] the United States Code also affords copyright owners with anti-circumvention protections. The Digital Millennium Copyright Act[94] (DMCA) states that "[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work."[95] Specifically, the DMCA makes it unlawful "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[96] Although the DMCA provides an exception for law enforcement activities,[97] it applies with full force to private actors, essentially incentivizing the creation of digital padlocks to protect copyrighted material and discouraging hackers from breaking those padlocks or casting unauthorized keys to them.[98]

---

works; (5) pictorial, graphic, and sculptural works; (6) motion pictures and other audiovisual works; (7) sound recordings; and (8) architectural works." § 102.

91. *See* Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) (opining that the purpose of "copyright law is to secure a fair return for an 'author's' creative labor . . . [and] to stimulate artistic creativity for the general public good").

92. *See* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 557 (1985) (highlighting that copyrights allow the author to "enjoy the right to market the original expression contained therein as just compensation for their investment"); *see also* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000), *aff'd*, 273 F.3d 429 (2d Cir. 2001) (noting that copyright owners "invest[] huge sums . . . in reliance upon a legal framework that, through the law of copyright, has ensured that they will have the exclusive right to copy and distribute those [works] for economic gain").

93. *See* 17 U.S.C. § 106 (granting the exclusive right to "reproduce," "prepare derivative works," or "distribute copies . . . of the copyrighted work").

94. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C. § 1201).

95. 17 U.S.C. § 1201(a)(1).

96. § 1201(a)(3)(A).

97. § 1201(e).

98. *See* Sanney, *supra* note 61, at 355–56 (detailing that the DMCA "allow[s] copyright owners to create these [digital rights management] locks to control how end users can access, copy, or convert information goods, such as software, music, movies, or books and restrict access to their works in order to protect those works

Copyright owners commonly secure their works with a digital padlock, using the DMCA's anti-circumvention provision as a backstop to prevent unauthorized access.[99] For example, motion picture companies place digital padlocks on DVDs to prevent the unauthorized copying of their movies.[100] These digital padlocks encrypt (or scramble) movies and permit only authorized hardware, such as DVD players, to decrypt (or unscramble) the movies for play.[101]

Smartphone manufacturers similarly employ the DMCA to protect their copyrights. One example involves the process coined "jailbreaking," in which hackers exploit flaws in Apple's iPhone software to install applications and modify the software without Apple's authorization.[102] To prevent this practice, the iPhone's software is imbedded with digital padlocks that prevent the unauthorized installation of programs, "forc[ing] both developers and consumers of iPhone applications to use the [Apple-run] App Store."[103] Essentially, Apple performs the role of gatekeeper: it controls the pool of programs available to consumers, not only to ensure payment but to maintain the company's high security standards.[104]

Although hackers who undermine these security standards by jailbreaking iPhones are circumventing a digital padlock, they do not necessarily violate the DMCA's anti-circumvention provision. Under the Act, Congress delegated to the Librarian of Congress the authority to establish rules defining the scope of the DMCA.[105] After

---

from infringement"). However, the Act also provides a "fair use" exception. *See* 17 U.S.C. § 107.

99. To prevail in a claim under the DMCA, a plaintiff "must prove: (1) ownership of a valid *copyright* on a work, (2) effectively controlled by a *technological measure*, which has been circumvented, (3) that third parties can now *access* (4) *without authorization*, in a manner that (5) infringes or facilitates infringing a right *protected* by the Copyright Act, because of a product that (6) the defendant . . . *designed or produced* primarily for circumvention." Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

100. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 308 (S.D.N.Y. 2000), *aff'd*, 273 F.3d 429 (2d Cir. 2001).

101. *Id.*

102. *See* Kevin Rogers, *Jailbroken: Examining the Policy and Legal Implications of iPhone Jailbreaking*, 13 PITT. J. TECH. L. & POL'Y 1, 1–4 (2013) (describing the technical aspects of jailbreaking).

103. Michael K. Cheng, Note, *iPhone Jailbreaking Under the DMCA: Towards a Functionalist Approach in Anti-Circumvention*, 25 BERKELEY TECH. L.J. 215, 220 (2010).

104. *See id.* at 221–24 (detailing the complexities of jailbreaking and the contentious "goal of [hackers to] defeat[] the iPhone's lock-in protections").

105. *See* 17 U.S.C. § 1201(a)(1)(C) (2012).

a contentious period that outlawed jailbreaking,[106] the Librarian of Congress issued a rule creating a very narrow exception to the DMCA's prosecutorial reach: the rule permits the jailbreaking of smartphones, but only to run "lawfully obtained software applications" or remove unwanted software that came preinstalled on the phone.[107] However, hackers may still be liable under the DMCA for circumventing digital padlocks protecting copyrighted material for purposes that do not fall into the Librarian of Congress's narrow rule, such as running software that Apple has not sanctioned.

B. Enforcing the Takings Clause Against the FBI

To determine whether a deprived property owner is owed just compensation under the Fifth Amendment, two inquiries are necessary. The federal government is constitutionally required to pay for the private property it appropriates only if (1) the taken item constitutes "property" under the Fifth Amendment, and (2) the government's conduct with the item constitutes a "taking" under the Fifth Amendment.[108] Under these inquiries, the federal government partially deprived Apple of its copyrighted software, a protected form of "property" under the Fifth Amendment, by creating technology to circumvent the passcode on the San Bernardino shooter's iPhone. Accordingly, it owes Apple "just compensation" for narrowing the scope of Apple's valid copyrighted software, jeopardizing the privacy of hundreds of millions of iPhone users, and thus diminishing Apple's competitive advantage based on its security.[109]

1. Apple's copyrighted software constitutes "property" under the Fifth Amendment

Although the Supreme Court has not yet determined whether certain intangible properties, such as copyrights, constitute "property" under the Fifth Amendment, copyright owners should

---

106. *See* Ezra Mechaber, *Here's How Cell Phone Unlocking Became Legal*, NAT'L ARCHIVES: OBAMA WHITE HOUSE (Aug. 15, 2014, 12:53 PM), https://obamawhitehouse.archives.gov/blog/2014/08/15/heres-how-cell-phone-unlocking-became-legal (explaining that 114,000 people signed an online petition calling to make cell phone jailbreaking legal after the Library of Congress entirely banned the practice).

107. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,953 (Oct. 28, 2015) (codified at 37 C.F.R. § 201.40(b)(4)).

108. *See supra* note 25 and accompanying text (outlining a proper takings analysis).

109. The magnitude of the federal government's diminution and the value of the "just compensation" owed to Apple is beyond the scope of this Note.

enjoy the same economic compensation that the Takings Clause affords owners of taken tangible property. First, numerous courts of appeals—particularly the First, Second, Fifth, Sixth, and Ninth circuits—have all suggested that copyrights satisfy the definition of property protected by the Fifth Amendment.[110] Moreover, the Supreme Court has recognized other forms of intangible property as "property" for Takings Clause purposes. In *Ruckelshaus v. Monsanto Co.*,[111] for example, the Court established that trade secrets constitute property, comparing trade secrets to "more tangible forms of property" because a "trade secret is assignable" and "can form the res of a trust."[112] Similarly, the Court has recognized other intangible property rights as property under the Takings Clause. Patent rights, for instance, have been considered "property" since the nineteenth century.[113] Copyrights also derive from statute, so they create precisely the same type of right as patents.[114] Because the Court has already recognized as property intangible rights such as trade secrets and patents, recognizing copyrights would be a natural extension and within the spirit of the Takings Clause.

Second, copyrights share many of the same attributes as other types of property recognized under the Takings Clause. Personal property undoubtedly falls within the purview of the Takings Clause,[115] and various bodies of law deem copyrights a form of "personal property." Under the Uniform Commercial Code, for instance, debtors can obtain credit by extending an interest in property, which includes

---

110. *See supra* notes 37–42 (citing decisions by various courts of appeals); *see also supra* note 43 (comparing positions of legal scholars on the issue).

111. 467 U.S. 986 (1984).

112. *See id.* at 1002–04.

113. *See, e.g.*, James v. Campbell, 104 U.S. 356, 358 (1881) (clarifying that patents "confer[] upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself, without just compensation, any more than it can appropriate or use without compensation land which has been patented to a private purchaser"); *see also* Christopher S. Storm, *Federal Patent Takings*, 2 J. BUS. ENTREPRENEURSHIP & L. 1, 7 (2008) (reviewing the Supreme Court jurisprudence and determining that the "historical evidence still weighs in favor of patents as constitutional property, even if the Supreme Court is not bound by such a finding").

114. *Compare* 35 U.S.C. § 154 (2012) (granting patent owners the right of exclusivity), *with* 17 U.S.C. § 106 (granting copyright owners the right of exclusivity).

115. *See* Horne v. Dep't of Agric., 135 S. Ct. 2419, 2425–28 (2015) (reassuring that "[t]he Government has a categorical duty to pay just compensation when it takes your car, just as when it takes your home," and holding that a crop of raisins fall within the purview of the Takings Clause).

both registered and unregistered copyrights.[116] In accordance with this notion, the Takings Clause should "protect[] 'private property' without any distinction between different types."[117]

Lastly, owners have no other recourse to remediate a governmental copyright infringement. Although some courts have maintained that the Takings Clause should not apply when the property owner has a statutory remedy,[118] copyright owners have no such remedy. A statutory remedy would exist under the DMCA if the hacker were a private citizen,[119] but no comparable remedy is available under the DMCA when the hacker is a sovereign or law enforcement authority.[120] Although Congress has expressly waived the federal government's sovereign immunity pertaining to copyright infringement generally,[121] courts have held that the federal government is immune from violations of the DMCA.[122] Because no

---

116. *See* U.C.C. § 9-102(a)(42) (AM. LAW INST. & UNIF. LAW COMM'N 1977) (defining general intangibles); *id.* § 9-109(a)(1) (identifying the scope of secured transactions as "a transaction . . . that creates a security interest in personal property"); *In re* World Auxiliary Power Co., 244 B.R. 149, 151, 156 (Bankr. N.D. Cal. 1999), *aff'd*, 303 F.3d 1120 (9th Cir. 2002) (discussing the proper method of filing for registered and unregistered copyrights under Article 9 of the Uniform Commercial Code). *See generally* Kenneth B. Axe, *Creation, Perfection and Enforcement of Security Interests in Intellectual Property Under Revised Article 9 of the Uniform Commercial Code*, 119 BANKING L.J. 62, 76–78 (2002) (discussing various issues pertaining to the perfection of general intangibles, such as copyrights).

117. *See Horne*, 135 S. Ct. at 2425 (holding that the "government's 'categorical duty' under the Fifth Amendment to pay just compensation when it 'physically takes possession of an interest in property'" applies to personal property (quoting Ark. Game & Fish Comm'n v. United States, 568 U.S. 23, 31 (2012)).

118. *See* Fla. Prepaid Postsecondary Educ. Expense Bd. v. Coll. Sav. Bank, 527 U.S. 627, 642 n.7 (1999) ("There is no suggestion . . . that Congress had in mind the Just Compensation Clause of the Fifth Amendment [when passing the Patent Remedy Act] . . . . [W]e think this omission precludes consideration of the Just Compensation Clause as a basis for the Patent Remedy Act."); Zoltek Corp. v. United States, 442 F.3d 1345, 1353 (Fed. Cir. 2006) (per curiam), *vacated*, 672 F.3d 1309 (Fed. Cir. 2012) (maintaining that plaintiffs cannot use the Takings Clause to receive just compensation if they also have a statutory remedy of patent infringement).

119. *See* 17 U.S.C. § 1203 (outlining civil remedies available).

120. *See id.* § 1201(e) (exempting "any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, [or] State").

121. *See* 28 U.S.C. § 1498(b) (waiving sovereign immunity "whenever the copyright in any work protected under the copyright laws of the United States shall be infringed by the United States, by a corporation owned or controlled by the United States, or by a contractor, subcontractor, or any person . . . acting for the Government and with the authorization or consent of the Government").

122. *See, e.g.*, Blueport Co., LLP v. United States, 71 Fed. Cl. 768, 781–82 (2006) (entertaining a claim for monetary damages against the United States, but holding

other remedy is available to copyright holders for governmental infringement, copyrights should constitute property under the Takings Clause of the Fifth Amendment to compensate victimized copyright owners from governmental interference.

2. FBI's hacking constitutes a "taking" under the Fifth Amendment

By shattering the digital padlock protecting Apple's copyrighted software, the federal government triggered the trip wire known as the Takings Clause, designed to deter tyrannical misappropriation. Though no "magic formula" exists to compute a governmental taking, one distinguishing characteristic is front and center in any analysis: deprivation of property. It follows that by forcibly circumventing Apple's encryption, the federal government partially deprived Apple of its copyrighted software and thus owes Apple "just compensation" for the deprivation.

a. Placing the FBI's conduct on the spectrum of governmental interference

Although concluding that the federal government deprived Apple of a portion of its valid copyrights is apparent, labeling such deprivation as a per se or *Penn Central* taking is much more opaque. The FBI narrowed the scope of Apple's available copyrights by essentially precluding Apple from fully-enforcing its copyrighted encryption method that protects users' information. Indeed, reasonable minds may differ on where to place the FBI's conduct on the spectrum of governmental interference. On the one hand, one may consider the FBI's conduct as a *Penn Central* taking because the state action merely diminished, rather than eviscerated, the economic value of Apple's software. Under this theory, each aspect of Apple's copyrights—the scope, length of time, enforcement mechanisms, etc.—is indivisible, so circumventing its encryption marginally decreases the overall value of the Apple iPhone software. In the proverbial bundle of sticks, rather than withdrawing a singular stick from Apple's bundle, the FBI has preserved each stick in the bundle but, through its hacking, has marginally devalued the entire bundle.

---

that "[t]here is no clear statement waiving sovereign immunity on the part of the government for claims arising under the DMCA"); *see also* John Timmer, *Air Force Cracks Software, Carpet Bombs DMCA*, ARS TECHNICA (Aug. 4, 2008, 2:02 PM), http://arstechnica.com/tech-policy/2008/08/air-force-cracks-software-carpet-bombs-dmca (noting that "the [*Blueport*] decision highlights the significant limits to the application of copyright law to the government charged with enforcing it").

On the other hand, one may observe the FBI's conduct as a per se taking because the state action eviscerated the economic value of a particular portion of Apple's software. Under this theory, each aspect of Apple's copyrights is divisible, so circumventing its encryption renders that aspect of Apple's copyrights—the aspect that allows Apple to fully-enforce its copyrighted encryption portion of its software—economically valueless. Rather than devalue the entire bundle of sticks, the FBI has withdrawn one of the sticks from the bundle entirely, rendering that singular stick valueless.

The distinction between per se and *Penn Central* takings here is nuanced but important in determining the FBI's liability under the Takings Clause. Deeming the FBI's conduct a *Penn Central* taking seems natural considering a copyright's abstract nature. But, this instinctual comfort derives from the mere fact that copyrights are a form of intangible property. Though copyrights fit comfortably in the *Penn Central* takings framework, courts are unfortunately more reluctant to find *Penn Central* takings compared to per se takings. Intangible property rights—such as copyrights, patents, and trade secrets—are vital to our society; although the Framers may not have conceived of intangible takings, courts should not hesitate to protect them from governmental intrusion.

b. Characterizing the FBI's conduct as a taking

Regardless of whether the analysis is steeped in *Penn Central* or per se takings jurisprudence, the federal government digitally trespassed on Apple's copyrighted property. Equivalent to a recorded deed for a house, Apple enjoys valid copyrights; it has the exclusive right to reproduce, recreate, alter, and distribute its iPhone software.[123] Like any house equipped with a lock on the front door, Apple encrypted its copyrighted software. That encrypted software protects a variety of security features: iPhones grant access to users only after the user correctly inputs a "user-determined, numeric passcode," and iPhones provide an optional setting that automatically erases all data after ten erroneous attempts at the passcode, a feature that is "fused into the phone."[124] However, the federal government circumvented Apple's encryption and created a "master key, capable of opening hundreds of millions of locks," essentially permitting anyone in the

123. *See* 17 U.S.C. §§ 102, 106; Apple iOS 9.0 Software, Copyright No. TX0008205229 (registered Sept. 16, 2015).

124. Apple's Motion to Vacate, *supra* note 74, at 5–6; Government's Ex Parte Application, *supra* note 5, at 3–5.

neighborhood to walk right through the front door and access users' most intimate information.[125]

Notwithstanding the fact that sovereign immunity protects the government from DMCA liability,[126] a proper analysis would conclude that the federal government, if acting as a private citizen, infringed Apple's copyrights, buttressing a governmental taking. Apple imbeds its iPhone software with digital padlocks—for example, the encryption that impeded the FBI's ability to bypass the user passcode on the phone at issue.[127] The DMCA proscribes any efforts to "bypass, remove, deactivate, or impair" any digital padlock to access copyrighted material.[128] Although the FBI has heavily censored the methodology that thwarted Apple's digital padlocks,[129] it seems likely that the FBI infringed Apple's copyrighted software. Considering that the encryption key was "fused into the phone,"[130] the hackers must have "bypass[ed], remove[d], or deactivate[d]" the software to gain access to the iPhone's storage.[131] Holding the federal government accountable for its hacking, therefore, is within the general spirit of the DMCA, which is to prevent hackers from circumventing digital padlocks protecting copyrighted material, such as Apple's copyrighted software.[132] Because Apple has no recourse under the DMCA, its only available option is to seek recompense under the Takings Clause; precluding such a remedy would result in arbitrary and unfettered governmental interference.

---

125. Apple's Motion to Vacate, *supra* note 74, at 3; *cf.* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 426 (1982) (finding a taking where a New York law requiring landlords to permit a cable television company to install some equipment on the roof was a "permanent physical occupation"). In its motion, Apple vowed that it would have had to "create a new version of the iPhone operating system designed to defeat the critical security features." Apple's Motion to Vacate, *supra* note 74, at 12. Thus, the federal government must have altered the iPhone's operating system to create the key to bypass its security features.

126. *See supra* note 122 and accompanying text.

127. *See* Apple's Motion to Vacate, *supra* note 74, at 5–6 (describing the iPhone's security features).

128. 17 U.S.C. § 1201(a)(3)(A). Furthermore, the jailbreaking exemption, discussed above, applies only to keys that allow the devices "to execute lawfully obtained software applications." *See* 37 C.F.R. § 201.40(b)(4) (2016).

129. *See* Tucker, *supra* note 84.

130. Government's Ex Parte Application, *supra* note 5, at 5.

131. *See* § 1201(a)(3)(A); Apple's Motion to Vacate, *supra* note 74, at 12 (opining that the FBI wanted Apple to modify the software to guarantee that the auto-erase function was turned off).

132. *See supra* Section III.A (discussing the characteristics of the DMCA).

Moreover, by readily *circumventing* Apple's encryption methods, the federal government is implicitly *devaluing* encryption devices, thereby narrowing the scope of Apple's options to enforce its copyrights. The government effectuates a taking when it prevents a property owner from exercising his legal rights attached to the property, affecting its present use and value.[133] In *Lucas*, for example, the Court found a taking when a law prohibited construction on beachfront property, thereby decreasing the market price of those beachfront lots.[134] Similarly, the FBI is devaluing encryption mechanisms by forcibly breaking the one protecting Apple's software. Encryption mechanisms protect information stored on smartphones with a digital padlock; although Congress and some state legislatures have proposed bills that would require tech companies to give law enforcement authorities a key to this padlock, none have become law.[135] While the law enforcement exception possibly indicates that Congress did not intend to provide a remedy under the DMCA, Congress cannot limit constitutional protections for property determined to be within the scope of the Takings Clause.

---

133. *Compare* United States v. Causby, 328 U.S. 256, 259, 267–68 (1946) (finding a government taking when military flight over a claimant's property caused the "destruction of the use of the property as a commercial chicken farm"), *with* Penn Cent. Transp. Co. v. New York City, 438 U.S. 104, 135 (1978) (finding no taking for a zoning decision because the "New York City law ha[d] in nowise impaired the present use of the Terminal").

134. *See* Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1007, 1081–82 (1992).

135. *See* 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 (outlining a U.S. Senate bill that "would make illegal the sort of user-controlled encryption that's in every modern iPhone"); *see also* Andrew Crocker, *Worried About Apple? California Has a Bill that Would Disable Encryption on All Phones*, ELECTRONIC FRONTIER FOUND. (Mar. 9, 2016), https://www.eff.org/deeplinks/2016/03/worried-about-apple-california-has-bill-would-disable-encryption-all-phones (criticizing a "new [California] State Assembly bill [that] would ban default encryption features on all smartphones"); Dennis Fisher, *New York Wants to Force Vendors to Decrypt Users' Phones*, ON THE WIRE (Jan. 13, 2016), https://www.onthewire.io/new-york-wants-to-force-vendors-to-decrypt-users-phones (discussing a New York state bill that would "require that smartphone manufacturers build mechanisms into the devices that would allow the companies to decrypt or unlock them on demand from law enforcement"). Moreover, Attorney General Jeff Sessions supports law enforcement's ability to circumvent encryption devices. *See* William Turton, *Trump's Attorney General Pick Wants to Give Cops Encryption Backdoors*, GIZMODO (Jan. 24, 2017, 9:27 AM), http://gizmodo.com/trumps-attorney-general-pick-wants-to-give-cops-encrypt-1791556095 (quoting Sessions during his confirmation process as stating that it is "critical . . . that national security and criminal investigators be able to overcome encryption").

The federal government is essentially choosing winners and losers by narrowing the scope of Apple's copyrighted software without legislation and affecting Apple's present-day value. Competition in the smartphone industry is fierce,[136] and the FBI jeopardized the vitality of Apple when it fundamentally undermined Apple's security. Apple sells a brand, not just a product, and its customers "have come to trust the Apple brand."[137] Hundreds of millions of people around the world store intimate and sensitive information on their iPhones: doctors store "confidential medical information," lawyers have "privileged communications with their clients," and common users save "financial information, emails, text messages, personal notes, reminders, [and] calendar appointments."[138] Lavabit, an email service prized for its security, filed an amicus brief in support of Apple and warned that a reputation for protecting users' privacy is important in this industry, describing the harm that the government caused when it previously breached Lavabit's secure email service.[139] Additionally, Hushmail, a provider of encrypted email, was "economically devastated" when the government breached

136. *See* Jack Linshi, *This 1 Chart Shows How Intense the Apple-Samsung Rivalry Really Is*, TIME (Apr. 29, 2015), http://time.com/3840414/samsung-apple-market-share (characterizing the competition between phone manufacturers Apple and Samsung as a "battle"); Manish Singh, *Samsung Gave Apple Stiff Competition in the US in 2015: Report*, GADGETS360 (Feb. 11, 2016), http://gadgets.ndtv.com/mobiles/news/samsung-gave-apple-stiff-competition-in-the-us-in-2015-report-801269 (explaining that "Apple's dominance in the United States may not last so long" and that other players, such as LG, Motorola, and HTC, are also growing); Ewan Spence, *Samsung Topples Apple as Galaxy S7 Defeats iPhone*, FORBES (May 4, 2016, 7:24 PM), http://www.forbes.com/sites/ewanspence/2016/05/04/samsung-overtakes-apple-us-smartphone-sales (reporting that "Samsung has reclaimed the top spot" for smartphone devices in the U.S. market).

137. Lavabit Brief, *supra* note 80, at 9.

138. *Id.* at 9, 11. Smartphones have a seemingly limitless capacity to store information; the Supreme Court has even said that "these devices are in fact minicomputers." Riley v. California, 134 S. Ct. 2473, 2489 (2014).

139. The FBI "sought to access encrypted e-mails stored on the Lavabit server, which were impossible to access without a user's password." Lavabit Brief, *supra* note 80, at 5. Lavabit explained that after the FBI acquired the "encryption key," it could "intercept, decrypt, inspect, and modify . . . all of [the] connections between Lavabit and the outside world" and access the target's data. *Id.*; *see also* Michael Phillips, *How the Government Killed a Secure E-Mail Company*, NEW YORKER (Aug. 9, 2013), http://www.newyorker.com/tech/elements/how-the-government-killed-a-secure-e-mail-company (describing the FBI's effort to break Lavabit's encryption because Edward Snowden, a former National Security Agency subcontractor who leaked classified information, sent an email from a Lavabit email address).

Hushmail's secured emails for investigative purposes.[140] Overall, the government's role in breaching technology security has reduced privacy, dwindled consumer confidence, and severely impacted the U.S. economy, costing security companies billions of dollars.[141] Further exacerbating the problem, the FBI is sharing this new master key with other law enforcement agencies, opening the floodgates that Apple predicted.[142] Foreign sovereigns—including China, Turkey, and Russia[143]—have requested the technology from the FBI, and so far the FBI has agreed to assist law enforcement authorities in Arkansas.[144] Because the federal government crafted and distributed a master key to the digital padlocks protecting Apple's copyrighted iPhone software and damaged Apple's reputation and competitive advantage, the FBI partially deprived Apple of its property and thus owes it "just compensation" for the diminution.[145]

---

140. *See* Lavabit Brief, *supra* note 80, at 11–12; *see also* Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED (Nov. 7, 2007, 3:39 PM), https://www.wired.com/2007/11/encrypted-e-mai (following the demise of Hushmail, who "market[ed] itself by saying that 'not even a Hushmail employee with access to our servers can read your encrypted e-mail,'" and detailing how it responded to a court order by "turn[ing] over 12 CDs worth of e-mails from three Hushmail accounts").

141. *See* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11, 15 (2015) (contending that "NSA programs, and public awareness of them, have had an immediate and detrimental impact on the U.S. economy . . . cost[ing] U.S. companies billions of dollars in lost sales" as consumers question their security and privacy).

142. *See* Apple's Motion to Vacate, *supra* note 74, at 24 (predicting that other agencies and governments would seek similar access to Apple's software).

143. *See* Serhat Kurt, *Turkey & Russia Want to Unlock iPhone of Russian Ambassador's Killer (Updated)*, MAC REPORTS (Dec. 22, 2016), http://macreports.com/turkey-russia-want-unlock-iphone-russian-ambassadors-killer ("Looking for leads on the terrorist's iPhone 4s, Turkish police and Russian authorities want to crack the PIN code on the device to access its content.").

144. Reena Flores, *FBI Pledges to Assist Local Police in Unlocking iPhones*, CBS NEWS (Apr. 2, 2016, 1:36 PM), http://www.cbsnews.com/news/fbi-pledges-to-assist-local-police-in-unlocking-iphones ("[T]he FBI offered their assistance [to local law enforcement agencies] in hacking the Apple phones in cases where they could provide evidence."); James Queally & Richard Winton, *FBI Agrees to Help Arkansas Prosecutors Open iPhone After Hack of San Bernardino Device*, L.A. TIMES (Mar. 31, 2016, 9:22 AM), http://www.latimes.com/local/lanow/la-me-ln-arkansas-fbi-phone-access-20160330-story.html ("Though the FBI might want to use the new tool to help solve other criminal cases, doing so would also make the process subject to discovery during criminal trials and place the information in the public domain . . . .").

145. *See* Horne v. Dep't of Agric., 135 S. Ct. 2419, 2425 (2015) (advising that the federal government has a "'categorical duty' under the Fifth Amendment to pay just compensation when it 'physically takes possession of an interest in property'" (quoting Ark. Game & Fish Comm'n v. United States, 133 S. Ct. 511, 518 (2012))).

CONCLUSION

The federal government seems to justify its hack because it is limited to "[j]ust this once" and "[j]ust this phone";[146] however, this is not the first time that it has sacrificed individual privacy, and this is not the first security mechanism that it has breached. Through its investigative arm, the federal government irreversibly destroyed the reputation of Lavabit, an email service prized for its security; it "economically devastated" Hushmail, a provider of encrypted emails;[147] it cost American businesses billions of dollars, crushing consumer confidence in certain products;[148] and it circumvented Apple's encryption software protecting sensitive information, such as financial records, family photos, and private emails.[149]

The federal government has consistently and deliberately chosen to sacrifice the individual liberties and privacy of hundreds of millions of Americans. In the last decade, the government has seemingly subscribed to the mantra that it is better to beg for forgiveness than ask for permission.[150] However, the government now seems to be shifting from an innocuous form of paternalism to a tyrannical form of taking, leaving those afflicted without a remedy.

By hacking Apple's digital padlocks protecting its copyrighted software, the FBI has unilaterally narrowed the scope of Apple's copyrighted property, thus qualifying as a "taking" and warranting "just compensation" prescribed by the Fifth Amendment of the U.S. Constitution. The FBI digitally trespassed onto Apple's copyrighted property and ostensibly prohibited encryption mechanisms for data, narrowing the scope of which Apple can enforce its copyrights. Moreover, the FBI has damaged Apple's reputation, injured its competitive advantage, and—most of all—jeopardized the sensitive information of hundreds of millions of iPhone users, now vulnerable

---

146. Apple's Motion to Vacate, *supra* note 74, at 3, *see also* Government's Ex Parte Application, *supra* note 5, at 4 (summarizing that the government sought Apple's help in accessing "the SUBJECT DEVICE *only*" (emphasis added)).

147. *See supra* notes 139–40 and accompanying text.

148. *See* Donohue, *supra* note 141, at 15.

149. *See supra* notes 137–45 and accompanying text.

150. *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112, 113 (2015) (arguing that intelligence legalism, simply asking whether a position is legal rather than practical, "gives systematically insufficient weight to individual liberty, and that its relentless focus on rights, and compliance, and law has obscured the absence of what should be an additional focus on interests, or balancing, or policy").

to hackers, identity thieves, hostile foreign agents, and unwarranted government surveillance.[151]

The Takings Clause compensates individuals for incurring private costs for the public benefit. The FBI circumvented Apple's encryption and altered the iPhone's security software to investigate a single criminal act. That alteration could be the master key that eventually empowers the FBI to open hundreds of millions of iPhones. Privacy advocates desire governmental transparency and accountability; security advocates desire governmental surveillance and strength. Our Constitution demands "just compensation" for the deprivation of property rights, and holding the government accountable for the economic damage it causes may provide a proper balance to these competing interests.

The Fifth Amendment's Takings Clause is a simple solution for a company deprived of its valid copyrights, yet its application could be the harvest that ends a remedial famine caused by governmental intrusion.[152] The FBI may have found the information it sought from the San Bernardino shooter, but in the future, the agency should consider in its calculus the economic consequences of such governmental intrusion. The government may have found the first bite of the Apple sweet, but it may come to find the second bite intolerably sour.

---

151. *See* Apple's Motion to Vacate, *supra* note 74, at 2–3.

152. *See* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1913) ("Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."); *see also* Cradle of Liberty Council, Inc. v. City of Philadelphia, 851 F. Supp. 2d 936, 953 (E.D. Pa. 2012) (interpreting Justice Brandeis' quotation and explaining "what he meant by that [quotation] is that when government action is exposed to the public when the public sees what's going on . . . the government tends to be on its best behavior").