A FIX FOR THE SMARTPHONE GLITCH: CONSUMER PROTECTION BY WAY OF LEGISLATIVE "KILL SWITCH"

WILLIAM P. SCHMITZ, JR.*

The sophistication and proliferation of advanced technology, particularly smartphones, has led to an increase in theft of these items. Companies created "kill switches" in hopes that this anti-theft method will protect smartphone customers. Lawmakers are scrambling to develop effective and relevant kill switch laws to curb this criminal activity. This Note addresses two recent legislative attempts, from Minnesota and California, and postulates that a hybrid of the two statutes is necessary to create a more comprehensive and useful tool to aid the government, technology companies, and consumers.

TABLE OF CONTENTS

* J. D. Candidate, Class of 2016, University of Illinois College of Law. I would like to thank Jamie Ward for her helpful feedback on an earlier draft of this Note. I would also like to thank Sarah Kimmer, Nick Pesavento, John Byers, Chris Jurmann, Carson King, and Nick Vallorano for their thoughtful advice and guidance throughout the writing process.

I. INTRODUCTION

As engineers and entrepreneurs rapidly develop a plethora of handheld electronic devices,[1] statutes and regulations controlling the manufacture of electronics, or lack thereof, are becoming increasingly antiquated.[2] Legislators have especially struggled to maintain relevant legislation regarding one of the primary technology booms of the past decade—the sophistication and proliferation of smartphone technology.[3] The benefits of smartphone technology are abundant, but according to multiple studies and law enforcement officials nationwide, smartphone theft is on the rise throughout the United States.[4] In response, some states are confronting the alarming trend of smartphone theft and related crime with legislation.[5]

State governments seeking to protect their citizens from smartphone theft have proposed, and in some cases passed, bills requiring smartphone manufacturers to integrate anti-theft solutions, dubbed "kill switches," into their products.[6] Among these is Minnesota, which enacted the first kill switch law nationwide in May 2014.[7] Shortly thereafter, in August 2014, California enacted the nation's second kill switch law.[8]

The Minnesota and California kill switch laws are the precursors to a wave of kill switch legislation that is sweeping the nation.[9] Other states,

1. *See* Jamie Carter, *Smartphone's Evolution Continues with a Raft of New Innovations*, S. CHINA MORNING POST (Mar. 15, 2013, 10:05 AM), http://www.scmp.com/lifestyle/technology/ article/ 1 190699/smartphones-evolution-continues-raft-new-innovations; *Have Smartphones Entered Their "Post-PC" Era?*, ENDEAVOUR PARTNERS (Oct. 2013), http://endeavourpartners.net/have-smartphones -entered-their-post-pc-era/ (noting smartphone "innovation continues to advance rapidly and perhaps even accelerate.").

2. Vivek Wadhwa, *Law and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 14, 2014), http://www.technologyreview.com/view/526401/laws-and-ethics-cant-keep-pace-with-technology/.

3. *Id.*

4. *See* OFFICE OF THE N.Y. STATE ATT'Y GEN., SECURE OUR SMARTPHONES INITIATIVE: ONE YEAR LATER 2 (2014) [hereinafter SECURE OUR SMARTPHONES]; Donna Tapellini, *Smart Phone Thefts Rose to 3.1 Million in 2013*, CONSUMERREPORTS.ORG (May 28, 2014, 4:00 PM), http://www. consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm; Martyn Williams, *Smartphones Driving Violent Crime Across US*, NETWORKWORLD (May 10, 2013, 6:22 PM), http://www.networkworld.com/article/2166191/ malware-cybercrime/smartphones-driving-violent-crime-across-us.html.

5. *See* Niraj Chokshi, *Minnesota Passes Nation's First Smartphone 'Kill Switch' Law*, WASH. POST (May 15, 2014), http://www.washingtonpost.com/blogs/govbeat/wp/2014/05/15/minnesota-passes-nations-first-smartphone-kill-switch-law/; Melody Gutierrez, *Gov. Brown Signs 'Kill Switch' Bill to Deter Smartphone Theft*, SFGATE (Aug. 26, 2014, 8:12 AM), http://www.sfgate.com/crime/article/Jerry-Brown-signs-kill-switch-bill-to-deter-5711452.php.

6. *See* Chokshi, *supra* note 5; Gutierrez, *supra* note 5.

7. *Governor Dayton Signs Smartphone "Kill Switch" Legislation, New Consumer Protection Law is First of its Kind in the Nation*, OFF. OF THE GOV. BLOG (May 14, 2014, 2:23 PM), http:// mn.gov/governor/blog/the-office-of-the-governor-blog-entry-detail.jsp?id=102-129588.

8. Richard Nieva, *California Governor Signs Smartphone 'Kill Switch' Bill into Law*, CNET (Aug. 25, 2014, 2:49 PM), http://www.cnet.com/news/calif-governor-signs-smartphone-kill-switch-bill/.

9. Gerry Smith, *New Legislation Would Require a 'Kill Switch' in Every Phone*, HUFF. POST (Mar. 3, 2014, 10:00 AM), http://www.huffingtonpost.com/2014/03/03/smartphone-theft-legislation _n_4886147.html; Gerry Smith, *U.S. Senator to Introduce 'Kill Switch' Legislation to Combat Phone*

such as Illinois and New York, have already proposed their own kill switch bills.[10] Furthermore, the Smartphone Theft Prevention Act, a federal kill switch bill, was introduced in February 2014.[11] These pioneering laws and bills have the potential to significantly affect the economy, smartphone manufacturing businesses, and the lives of over 145 million consumers.[12] The question remains as to whether kill switch legislation is necessary to combat the smartphone theft epidemic, and if so, what specific legislative approach should be taken.

This Note contends, first, that kill switch legislation should be pursued, and second, that Congress should enact a federal kill switch law featuring a blend of the legislative approaches taken in Minnesota and California. Part II of this Note investigates the global smartphone black market, surging smartphone related crime trends in the United States, and the capabilities of kill switch technology. Part III then evaluates the legislative approaches taken in Minnesota and California. Additionally, Part III assesses how kill switch legislation might affect innovation in the smartphone industry and surveys two federal bills aimed at combatting smartphone theft. Part IV of this Note recommends a federal kill switch law that blends the legislative approaches taken in Minnesota and California. Part V briefly concludes.

II. BACKGROUND

A smartphone is commonly defined as "a cell phone that includes additional software functions."[13] Modern smartphone technology is relatively new; although IBM designed a primitive smartphone in 1993.[14] The Apple iPhone, currently the best-selling smartphone on the market,[15] was launched less than a decade ago in 2007.[16]

A. Smartphones are Portable, Popular, and Pricey

By their very nature, smartphones are highly portable, sophisticated devices.[17] From the time smartphones were invented and first marketed

Thefts, HUFF. POST (Jan. 23, 2014, 6:59 PM), http://www.huffingtonpost.com/ 2014/01/23/legislation-phone-thefts_n_4653392.html.

10. S. 3539, 98th Gen. Assemb., Reg. Sess. (Ill. 2014); S. 51, 201st Leg., Reg. Sess. (N.Y. 2015).

11. H.R. 4065, 113th Cong. (2014).

12. *See* WILLIAM DUCKWORTH, ANTI-THEFT SOFTWARE IN MOBILE PHONES COULD SAVE CONSUMERS $2.6B A YEAR 1 (2014).

13. *Smartphone Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary /smartphone (last visited Sept. 7, 2015).

14. William L. Hosch, *Smartphone*, ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/ EBchecked/topic/1498102/smartphone (last updated Oct. 3, 2013).

15. *Apple and Samsung Dominate List of Top 10 Best-Selling Smartphones*, YAHOO! (July 17, 2014, 6:08 AM), http://news.yahoo.com/apple-samsung-dominate-list-top-10-best-selling-100853996.html.

16. Mathew Honan, *Apple Unveils iPhone*, MACWORLD (Jan. 9, 2007, 1:55 PM), http://www.macworld.com/article/1054769/iphone.html.

17. *See Protecting Portable Devices: Physical Security*, U.S. COMP. EMERGENCY READINESS TEAM (Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/st04-017.

to the public, they gained tremendous popularity, and the number of users is growing rapidly.[18] Worldwide, only an estimated five percent of the global population owned a smartphone in 2009.[19] Smartphone ownership is expected to multiply seven times over by 2016, to about thirty-five percent of the global population.[20] To put that figure into perspective, it is approximately 2.5 billion people—roughly equal to the populations of China and India combined.[21] On the home front, over three quarters of people in the United States, ages fifteen to sixty-four, or a whopping seventy-eight percent of all adult Americans, reported using a smartphone in 2012.[22] According to another more recent estimate, over 145 million Americans owned a smartphone in 2014.[23]

Not only are smartphones popular and portable, the devices are also considerably valuable.[24] "For many of us, these devices are among our most valuable possessions. Or, at the very least, they are among the most valuable possessions that we cart with us everywhere we go."[25] Smartphone value, to some, is much higher than sheer price: smartphones can hold family photos, personal and business contacts, bank account balances, work emails, other private information.[26] Base value, the average price of an unlocked "cheap" smartphone is about $398, and most smartphones are even pricier.[27] Thus, it is no surprise that smartphones are an attractive target for thieves—the devices are ingeniously portable, wildly popular, and undeniably pricey.[28]

B. The Emerging Global Smartphone Black Market

Due to widespread use and relatively high value, a massive global black market[29] for smartphones has developed.[30] Indeed, a stolen smartphone is "worth 13 times more, per ounce, *than a block of silver*," and "can be swiped, wiped, and resold for hundreds of [dollars] in the

18. Henry Blodget, *Actually, the US Smartphone Revolution has Entered the Late Innings*, BUS. INSIDER (Sept. 13, 2012, 9:23 AM), http://www.businessinsider.com/us-smartphone-market-2012-9.

19. Matthew Shaer, *The Secret World of Stolen Smartphones, Where Business is Booming*, WIRED (Dec. 18, 2014, 6:30 AM), http://www.wired.com/2014/12/where-stolen-smart-phones-go/.

20. *Id.*

21. *Id.*

22. Blodget, *supra* note 18.

23. DUCKWORTH, *supra* note 12, at 2.

24. Lauren Pack, *Popularity, Price Makes Smartphones Top Pick Among Thieves*, JOURNAL-NEWS (June 1, 2014, 8:00 AM), http://www.journal-news.com/news/news/crime-law/popularity-price-make-smartphones-top-pick-among-t/nf92d/.

25. Shaer, *supra* note 19.

26. *Id.*

27. Tristan Louis, *The Real Price of a Smartphone*, FORBES (Sept. 14, 2013, 3:09 PM), http://www.forbes.com/sites/tristanlouis/2013/09/14/the-real-cost-of-a-smartphone/.

28. *See* Pack, *supra* note 24.

29. *Black Market Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/ dictionary/black%20market (last visited Sept. 7, 2015) (defining a black market as an "illicit trade in goods or commodities in violation of official regulations.").

30. Gerry Smith, *Inside the Massive Global Black Market for Smartphones*, HUFF. POST (July 22, 2013, 5:34 PM), http://www.huffingtonpost.com/2013/07/13/smartphone-black-market_n_3510341.html.

space of an hour . . . ."[31] Stolen smartphones can be worth more than a stolen wallet, and often can be resold on the black market for more than a stolen tablet or laptop.[32] Thus, smartphones are a tremendously hot commodity among black market dealers and street thieves alike.[33]

Fueled by an influx of stolen devices, illegitimate vendors on the black market are able to take advantage of dramatic disparity between U.S. and foreign smartphone prices, and peddle smartphones originating in the United States for hundreds and even thousands of dollars.[34] "The plots coming to light today are complex, and increasingly global."[35] Even terrorist organizations are exploiting smartphone black markets.[36] In 2009, federal agents charged Hezbollah operatives with attempting to purchase thousands of stolen devices in Philadelphia.[37] The purchases were part of a larger scheme to ship phones to the United Arab Emirates and Hong Kong to generate funds for Shiite militias.[38]

Brazil offers prime example of how smartphone black markets can be such a lucrative enterprise.[39] Domestic electronics prices have skyrocketed in Brazil due to high taxes and import tariffs.[40] Sixteen percent import tariffs and other taxes comprise over a third of the retail price for smartphones, tablets, and other electronics in Brazil.[41] The result is outrageously high smartphone prices, such as $1100 for a Samsung Galaxy S4.[42] Unsurprisingly, Brazilian consumers are readily looking for alternative vendors to meet their electronics needs.[43] The opportunity to sell smartphones below market prices and still turn a profit has enticed Chinese, Lebanese, and Syrian dealers, among others, to participate in the Brazilian underground smartphone trade.[44] The supply of smartphones driving underground trade comes largely from the United States.[45]

A culture of consumerism in the United States provides a steady flow of smartphones to thieves.[46] The problem is exacerbated by subsidized smartphone prices allowing U.S. consumers to purchase devices at

31. Shaer, *supra* note 19 (emphasis added).
32. DUCKWORTH, *supra* note 12, at 1.
33. *Id.*
34. Smith, *supra* note 30.
35. Ilya Marritz, *Understanding the Smartphone Black Market*, WNYC (Sept. 11, 2013), http://www.wnyc.org/story/317187-black-market-stolen-smartphones/.
36. Smith, *supra* note 30.
37. *Id.*
38. *Id.*
39. *See* Amar Toor, *The World's Most Expensive Smartphone: Brazil's Black Market for Gadgets is Booming*, VERGE (July 30, 2013, 1:45 PM), http://www.theverge.com/2013/7/ 30/4571602/brazil-inflation-fuel-black-market-for-smuggled-smartphones-tablets.
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*
44. *Id.*
45. *See* Shaer, *supra* note 19.
46. Jenny Kido, *When the Habit of Serial-Buying Smartphones Goes Wrong—a Father's Tale*, XNSPY (Dec. 30, 2014), http://xnspy.com/blog/when-the-habit-of-serial-buying-smartphones-goes-wrong-a-fathers-tale.html.

a fraction of their value by agreeing to a contract with a carrier.[47] According to Marci Carris, Vice President of Customer Finance Services at Sprint, "[p]hones stolen in the United States have been located on all continents except Antarctica."[48]

C. Rising Smartphone Related Crime Rates in the United States

Both abroad and in the United States, steady demand and huge profits incentivize criminals to participate in the stolen smartphone trade. More than 1.6 million Americans fell victim to smartphone theft in 2012 alone.[49] In a year's time, that number reportedly almost doubled, to roughly 3.1 million smartphone thefts in 2013.[50] Lookout, a mobile security firm, asserts that as many as one in ten U.S. users have had their smartphone stolen, and sixty-eight percent never recovered their device.[51]

Smartphone theft is especially pervasive in large cities.[52] Disturbingly, these crimes are also associated with growing levels of violence: "[I]n just over half the incidents [in 2013], victims were punched, kicked or otherwise physically intimidated for their phones, and in a quarter of robberies, users were threatened with guns or knives."[53]

San Francisco, for instance, has experienced a substantial surge in smartphone related crime.[54] According to an FBI Uniform Crime Report, violent crime increased by 7.5 percent and property crime increased by 18.3 percent in the Bay Area during 2012.[55] Both spiked another ten percent the following year in 2013.[56] The San Francisco Police Department attributes the increase in crime in large part to "increases in the theft or robbery of cell phones."[57]

San Francisco's case is not unique; the smartphone crime epidemic is escalating in many major cities.[58] For example, Denver experienced a twenty-two percent hike in iPhone theft in 2013 compared to the previous year.[59] Meanwhile in New York City, cellphone theft accounted for over half of all street crime within city limits in 2013.[60] Also, the number of thefts involving Apple products increased by eight percent during the

47. Smith, *supra* note 30.
48. *Id.* (original quotations omitted).
49. *Id.*
50. Gerry Smith, *Smartphone Thefts Rose in 2013 Despite New Push to Stop Them*, HUFFINGTON POST (Jan. 15, 2014, 1:03 PM), http://www.huffingtonpost.com/2014/01/15/ smartphone-thefts-2013 _n_4598399.html.
51. Shaer, *supra* note 19.
52. Smith, *supra* note 50.
53. Williams, *supra* note 4.
54. *See id.*
55. Parker Yesko, *Smartphones Trigger Rise in Crime Rate as New iPhone Features a Fingerprint Lock*, SFBG (Sept. 10, 2013, 12:26 PM), http://www.sfbg.com/politics/2013/09/10/ smartphones-trigger-rise-crime-rate-new-iphone-features-fingerprint-lock.
56. *Id.*
57. *Id.*
58. Williams, *supra* note 4.
59. Smith, *supra* note 50.
60. Williams, *supra* note 4.

same period, marking the second year in a row of major "Apple Picking"[61] growth. In Kansas City, cellphone thefts rose twenty percent from 2009 to 2013.[62] In Philadelphia, the Southeastern Pennsylvania Transportation Authority (SEPTA) reported smartphone theft rose a disquieting forty-four percent from 2011 to 2013.[63] In Washington D.C., the number of robberies involving a smartphone was fifty-four percent higher in 2011 than in 2007,[64] the year the original iPhone was released.[65]

D. Kill Switch Technology

A proposed solution to combat smartphone theft is to integrate kill switch technology into smartphones.[66] Kill switch technology enables victims of smartphone theft to disable their stolen smartphones and wipe their data from a remote location.[67] Additionally, kill switch technology allows people with lost or stolen smartphones to delete contacts, photos, email, and other personal information.[68]

Kill switch technology comes in multiple varieties.[69] Hard kill switches render a smartphone permanently inoperable, reducing it a piece of hardware with little value other than that what can be salvaged by selling its parts.[70] Smartphones that have been shut down by a hard kill switch, known as "bricking," can never be used again regardless of user.[71] Another type of kill switch, more common among those offered by private developers and included in kill switch legislation, is referred to as a soft kill switch.[72] Soft kill switches are preferable to most consumers, because they do not render the device permanently inoperable.[73] Even after engaging a soft kill switch, authorized users who recover the smartphone may retroactively disarm the switch and reactivate the device.[74]

Kill switches also come in two classes related to how and when they are equipped.[75] Opt-in kill switches are equipped as a result of a consum-

61. Rolfe Winkler, *Fighting the iCrime Wave*, WALL ST. J. (July 27, 2012, 9:00 PM), http://online.wsj.com/news/articles/SB10000872396390443931404577550823904439852.

62. Matt Campbell, *Calls Grow Louder for 'Kill Switches' to Deter Smartphone Theft*, KAN. CITY STAR (May 19, 2014, 10:57 PM), http://www.kansascity.com/news/business/technology/article376042/Calls-grow-louder-for-%E2%80%98kill-switches%E2%80%99-to-deter-smartphone-theft.html.

63. Smith, *supra* note 50.

64. Winkler, *supra* note 61.

65. Honan, *supra* note 16.

66. *See* Doug Gross, *'Kill Switch' may be Standard on U.S. Phones in 2015*, CNN (Apr. 16, 2014, 5:26 PM), http://www.cnn.com/2014/04/16/tech/mobile/ctia-phone-kill-switch/.

67. *Id.*

68. *Id.*

69. *See* Brad Molen, *The Government Shouldn't Regulate Smartphone Kill Switches*, ENGADGET (Aug. 18, 2014, 3:30 PM), www.engadget.com/2014/08/18/cellphone-kill-switch/.

70. *See id.*

71. *Id.*

72. *Id.*

73. *See id.*

74. *Id.*

75. *See id.*

er actively deciding to download or turn on a kill switch function on their mobile device.[76] Conversely, opt-out kill switches are already equipped in the default settings of a smartphone sold at retail.[77] In the opt-out scenario, a consumer must consciously disarm or turn off the function if they do not wish to employ use of the kill switch on their mobile device.[78]

1. Promoting Kill Switch Technology

Advocates of kill switch technology, including law enforcement officials, assert that it will protect personal information and discourage thieves because the stolen smartphones will be rendered useless.[79] Proponents contend that integrating kill switches into smartphones can decrease smartphone theft because "[i]f all stolen phones could easily be disabled, criminals would have virtually no incentive to steal a phone in the first place."[80]

The public seems receptive of smartphone kill switch technology; indeed, most consumers want it to be implemented.[81] A Consumer Opinion Survey regarding smartphone kill switch technology was conducted in February 2014 that inquired a demographically weighted, representative sample of 1,200 smartphone users.[82] The results indicate that consumers, the would-be victims of smartphone theft, are overwhelmingly in favor of kill switch technology and believe it could decrease crime.[83] According to the survey, "83% of smartphone owners believe that a [k]ill [s]witch would reduce cell phone theft"[84] and "99% of smartphone owners feel wireless carriers should give all consumers the option to disable a cell phone if it is stolen."[85]

By decreasing theft, kill switches could help consumers financially as well.[86] According to the Federal Communications Commission, replacing lost and stolen phones cost consumers an estimated $30 billion in 2012; a figure that could be significantly reduced if kill switches are effective.[87] Consumers also spend $4.8 billion annually on carrier-provided premium insurance plans.[88] According to a study by William Duckworth, a business professor at Creighton University and a staunch consumer advocate, if kill switch technology were mandatory in all phones, many con-

76. *Id.*
77. *Id.*
78. *Id.*
79. Gross, *supra* note 66.
80. DUCKWORTH, *supra* note 12.
81. *See id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. Press Release, Creighton Univ., Creighton Professor Releases Research on Mobile Phone Kill Switch (last visited Sept. 7, 2015), *available at* https://business.creighton.edu/news/ creighton-professor-releases-research-mobile-phone-kill-switch.
87. *See* Campbell, *supra* note 62.
88. DUCKWORTH, *supra* note 12.

sumers would switch to basic smartphone insurance.[89] With less money spent on premium insurance coverage, consumers could save about $2 billion annually.[90] Therefore, advocates of kill switch technology posit that kill switches will decrease smartphone theft, thereby saving consumers billions of dollars.

2. Challenging Kill Switch Technology

Notwithstanding apparent public approval, kill switch technology is not universally accepted as the most prudent way to combat smartphone theft.[91] Due to the capability of kill switch technology to disable smartphones, adversaries maintain that the risk of misuse by carriers and law enforcement outweighs any potential to increase safety.[92] For instance, law enforcement might disable the phones of reporters who tweet pictures from a crime scene, encroaching on rights free speech and free press.[93] Kill switch opponents also fear hackers might shut down smartphones that have not been lost or stolen, which could be especially dangerous if the smartphones were disabled during emergencies or crises.[94] Moreover, other opponents of smartphone kill switch technology argue kill switch legislation is "unnecessary, due to existing software like Find My iPhone and Android Device Manager, as well as stolen smartphone databases."[95]

3. Private Sector Perspectives

a. Past Success in the Private Sector: Automobile Theft Reduction

The smartphone theft epidemic has been likened to the rise of automobile thefts that peaked in the early 1990s.[96] According to the National Insurance Crime Bureau, there were about 328,200 automobile thefts in 1960, which equates to roughly 182 thefts per 100,000 people.[97] By 1991, the number of automobile thefts rose to a historic high of about

89. *Id.*

90. *Id.*

91. CELLULAR TELECOMM. INDUS. ASS'N, WHY A "KILL SWITCH" ISN'T THE ANSWER, *available at* http://files.ctia.org/pdf/Why_a_Kill_Switch_Isn_t_the_Answer.pdf.

92. *Id.*

93. Jonathan Peters, *Why California's Smartphone 'Kill Switch' Law Should Concern Journalists*, COLUM. JOURNALISM REV. (Sept. 4, 2014), http://www.cjr.org/united_states_project/california_smartphone_kill_switch_law_concerns_for_journalists.php?page=all.

94. *See* CELLULAR TELECOMM. INDUS. ASS'N, *supra* note 91.

95. Sean Hollister, *First Smartphone 'Kill Switch' Law Signed in Minnesota*, VERGE (May 14, 2014), http://www.theverge.com/2014/5/14/5718910/first-smartphone-kill-switch-law-signed-in-minnesota.

96. *See* SECURE OUR SMARTPHONES, *supra* note 4, at 7.

97. *Historical Look at Vehicle Theft in the U.S.*, NAT'L INS. CRIME BUREAU, https://www.nicb.org/newsroom/news-releases/historical-look-at-vehicle-theft-in-the-u-s- (last visited Sept. 7, 2015) [hereinafter NAT'L INS. CRIME BUREAU].

1,661,738 thefts, or 659 thefts per 100,000 people.[98] Thus, automobile theft rates increased approximately 262 percent over three decades.[99]

In response, the automobile industry collaborated with law enforcement, joining technology, "the great equalizer,"[100] with painstaking police work.[101] Manufacturers introduced—and law enforcement benefitted from—technical anti-theft solutions such as "transponder keys, immobilizing devices, [and] vehicle tracking devices."[102] These efforts proved effective, and automobile thefts have steadily declined since the early 1990s.[103] By 2013, the number of automobile thefts diminished to levels not seen since 1967.[104] Thus, the private sector was able to integrate technological solutions successfully, thereby increasing public safety by reducing automobile theft, without government direction.

b. Kill Switches in the Private Sector

Many major smartphone carriers and manufacturers originally took up an anti-kill switch position.[105] According to the Secure Our Smartphones coalition, the smartphone industry already had the capability to integrate kill switches and other anti-theft solutions since at least early 2013.[106] Yet, smartphone manufacturers and carriers did not offer those options at that time. Most firms have since converted their allegiance and pledged to incorporate kill switch technology in their products.[107] In anticipation of the first kill switch law being passed in Minnesota, a number of companies signed on to a voluntary initiative to provide basic kill switch capabilities to their users.[108] Companies who signed the initiative include Apple, Asurion, AT&T, Google, HTC, Huawei, LG, Motorola Mobility, Microsoft, Nokia, Samsung, Sprint, T-Mobile, U.S. Cellular, and Verizon Wireless.[109]

Anti-theft features offered by most smartphone companies are of the opt-in, soft kill switch variety.[110] Depending on their smartphone carrier and manufacturer, many consumers can opt-in to equip their smartphones with remote locking, tracking, and wiping capabilities—the

98. *Id.*

99. To determine the percent increase, the absolute value of the difference (659 thefts per 100,000 people minus 182 thefts per 100,000 people) is divided by the original value (182 thefts per 100,000 people). The difference of 477 thefts per 100,000 people, divided by the original value of 182 thefts per 100,000 people, is equal to a quotient of 2.62. Thus, the theft increase is 262 percent.

100. NAT'L INS. CRIME BUREAU, supra note 97.

101. *See* SECURE OUR SMARTPHONES, *supra* note 4, at 15.

102. *Id.* at 7.

103. *Id.*

104. *See* NAT'L INS. CRIME BUREAU, *supra* note 97.

105. Gross, *supra* note 66.

106. *See* SECURE OUR SMARTPHONES, *supra* note 4, at 7.

107. Gross, *supra* note 66.

108. *See* Chokshi, *supra* note 5.

109. *Id.*

110. *See* Molen, *supra* note 69.

basic functions of a kill switch.[111] Furthermore, once a consumer decides to opt-in, private companies offer an abundance of applications and other anti-theft solutions.[112] Though some require payment of a fee, many options are available free of charge.[113] Dozens of options are compatible with major smartphone operating systems including Android,[114] Blackberry,[115] iOS,[116] Symbian,[117] and Windows.[118]

i. Apple's Activation Lock

Industry leader Apple was the first to develop kill switch functions in the private sector and has offered Activation Lock since September 18, 2013.[119] Activation Lock is a kill switch package available to iPhone consumers so long as they have an iPhone with the iOS 7 operating system installed.[120] Essentially, consumers who simply enable the program in their phone settings will obtain basic kill switch functionality.[121]

Thus far, the upshots of Apple's introduction of Activation Lock seem to confirm the effectiveness of kill switch technology in deterring smartphone theft.[122] According to a crime report studying a five-month timespan proximately following the release of Activation Lock, "the theft of Apple devices *fell* by 17 percent in New York City, while thefts of Samsung products *increased* by 51 percent compared to the same time period in the previous year."[123] Over the same period, the trend in New

111. Microsoft et. al, *Re: SB 962 Letter of Concern; Not the Solution for Smartphone Theft*, CTIA, http://www.ctia.org/docs/default-source/Legislative-Activity/coalition-letter-of-concern-in-response-to-california-senate-bill-962-regarding-smartphone-theft.pdf?sfvrsn=0 (last visited Sept. 7, 2014) [hereinafter Microsoft Letter].

112. *See Anti-theft Protection Apps for Android Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-android-wireless-handsets (last visited Sept. 7, 2015) [hereinafter *Android Wireless*]; *Anti-theft Protection Apps for iOS (Apple) Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-ios-%28apple%29-wireless-handsets (last visited Sept. 7, 2015) [hereinafter *Apple Wireless*]; *Anti-theft Protection Apps for BlackBerry Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-blackberry (last visited Sept. 7, 2015) [hereinafter *BlackBerry Wireless*]; *Anti-theft Protection Apps for Symbian Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-symbian-wireless-handsets (last visited Sept. 7, 2015) [hereinafter *Symbian Wireless*]; *Anti-theft Protection Apps for Windows Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-windows-wireless-handsets (last visited Sept. 7, 2015) [hereinafter *Windows Wireless*].

113. *See Android Wireless*, *supra* note 112; *Apple Wireless*, *supra* note 112; *BlackBerry Wireless*, *supra* note 112; *Symbian Wireless*, *supra* note 112; *Windows Wireless*, *supra* note 112.

114. *See Android Wireless*, *supra* note 112.

115. *See BlackBerry Wireless*, *supra* note 112.

116. *See Apple Wireless*, *supra* note 112.

117. *See Symbian Wireless*, *supra* note 112.

118. *See Windows Wireless*, *supra* note 112.

119. SECURE OUR SMARTPHONES INITIATIVE, *supra* note 4, at i.

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.* at ii.

York City was simulated in London.[124] Likewise, in San Francisco, the report indicated a decline in iPhone robberies by thirty-eight percent, while the city experienced an increase in the theft of smartphones produced by other manufacturers.[125]

ii. Anti-theft Solutions by Samsung, Microsoft, and Google

Fortunately for consumers who do not own an iPhone, Samsung followed suit and designed a kill switch solution of its own.[126] Revealed on April 5, 2014 and offered for the Samsung Galaxy line of smartphones, this kill switch option is called Reactivation Lock.[127] Microsoft and Google soon joined the smartphone kill switch initiative as well.[128] On June 19, 2014, Microsoft confirmed that it would include anti-theft technological solutions for Windows Phone operating systems, which are featured in Nokia smartphones.[129] Google similarly promised to create a kill switch option for Android operating systems.[130] Google's commitment is critical for a substantial number of smartphone users, as Android is currently the most prevalent smartphone operating system worldwide.[131]

c. Miscellaneous Efforts in the Private Sector

Apart from developing kill switches, the smartphone industry has collaborated with law enforcement and the Federal Communications Commission to combat smartphone theft with other initiatives.[132] For example, the Cellular Telecommunications Industry Association created a website and released a public service announcement video to guide consumers through the process of equipping their smartphones with existing anti-theft apps and programs.[133] Additionally, efforts to establish databases, educational programs, international partnerships, and other solutions have facilitated the ability of law enforcement to track and locate stolen smartphones.[134]

4. Public Sector Platforms

Whereas significant strides are being made in the private sector, voluntary performance in the growing smartphone kill switch initiative is

124. *Id.*
125. *Id.*
126. *Id.* at i.
127. *Id.*
128. *Id.* at ii.
129. *Id.*
130. *Id.*
131. *Id.*
132. Microsoft Letter, *supra* note 111.
133. *See How to Deter Smartphone Thefts and Protect Your Data*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data (last updated June 2015) (outlining preventative measures smartphone consumers can take to lock, track, and safeguard personal information in the event their device is lost or stolen).
134. Microsoft Letter, *supra* note 111.

considered insufficient to some lawmakers.[135] Despite pledges by manufacturers and wireless carriers to integrate kill switches into their products, California state Senator Mark Leno responded, "[t]oday's 'opt-in' proposal misses the mark if the ultimate goal is to combat street crime and violent thefts involving smartphones."[136]

Despite more and more smartphones being *capable* of kill switch technology through private solutions, some government actors contend that "the majority of smartphones still [are] without an *active* kill switch, [and] smartphone-related thefts and violence remain a tragic reality."[137] Unsatisfied, some lawmakers have introduced kill switch bills. Several states have already passed smartphone kill switch laws.[138] On May 24, 2014, Minnesota passed the first kill switch law in the United States.[139] Soon thereafter, on August 25, 2014, California passed its own kill switch law.[140]

III. ANALYSIS

Confronting the smartphone theft epidemic is no easy task. A cure seems elusive, in part, because smartphone technology is in constant flux and thieves regularly adapt. Minnesota and California, however, believe they have found an antidote: kill switch laws.[141] Yet, great uncertainty remains regarding this experimental new brand of legislation: should kill switch legislation be enacted at all? What specific attributes or provisions formulate an ideal kill switch law? Can kill switch laws be implemented without overly burdening the smartphone industry or stifling innovation? Furthermore, should kill switch laws be pursued on a state-by-state basis, or should the federal government create a national standard? These questions are addressed later in this Note.[142]

To establish a model legislative approach that balances competing government and private interests, deters thieves, and does not stifle innovation, this Part of the Note proceeds with three stages of analysis. First, it dissects the legislative approaches taken in Minnesota and California, in order to determine what specific provisions comprise an ideal smartphone kill switch law. Second, it attempts to determine what effect, if any, kill switch legislation will have on innovation in the smartphone industry. Third, it briefly surveys two federal smartphone bills—a kill switch bill and another anti-theft bill—to consider what advantages a federal legislative approach might offer.

135. *See* Gross, *supra* note 66.
136. *Id.*
137. SECURE OUR SMARTPHONES, *supra* note 4, at ii (emphasis added).
138. *See* Chokshi, *supra* note 5.
139. *Id.*
140. Gutierrez, *supra* note 5.
141. *See* Chokshi, *supra* note 5; Gutierrez, *supra* note 5.
142. *See* discussion *infra* Parts III, IV.

A. Smartphone Kill Switch Legislation at the State Level

Numerous states across the United States have considered or are considering smartphone kill switch legislation, including Illinois,[143] Mississippi,[144] Nevada,[145] New York,[146] New Jersey,[147] and Rhode Island.[148] Minnesota and California are the first two states to officially enact kill switch laws.[149] Though both Minnesota and California aim to combat the smartphone theft epidemic, their respective kill switch laws are markedly distinct.

1. Minnesota's Kill Switch Law

Given that Minnesota's kill switch law is the first of its kind, it is appropriate that it may serve as a baseline with which other kill switch laws and bills may be compared.[150] Minnesota's kill switch law, effective July 1, 2015, originated as SF1740 in the Minnesota Senate and was first introduced on February 25, 2014.[151] Calling for kill switches of the opt-in, soft variety, the Minnesota kill switch bill consists of two articles.[152] Article 1 pertains to smartphone anti-theft protection, whereas Article 2 focuses on secondary market transactions.[153] Thus, Minnesota took a dual-threat legislative approach in its attempt to curb smartphone theft and protect consumers. In order to appreciate the worth of Minnesota's approach, that is coupling kill switch requirements with smartphone resale restrictions,[154] it is helpful to examine each article of SF1740, as codified in the Minnesota Statutes, individually.

a. Smart Phone Anti-theft Protection

Article 1 of SF1740, titled "Smart Phone Antitheft Protection," was codified as 325F.698 in the 2014 Minnesota Statutes ("Section 698").[155] Its

143. S. 3539, 98th Gen. Assemb., Reg. Sess. (Ill. 2014).

144. Jimmie E. Gates, *Mississippi Smartphones: "Kill Switch" Bill*, CLARION-LEDGER (Jan. 14, 2015, 8:45 AM), http://www.clarionledger.com/story/politicalledger/2015/01/13/smartphone-kill-switch-derrick-simmons/21694411/.

145. Anjeanette Damon, *States, Privacy Advocates Battle over Phone 'Kill Switch,'* USA TODAY (Oct. 22, 2014), http://www.usatoday.com/story/news/nation/2014/10/22/cellphone-kill-switch/17749759/.

146. S. 51, 201st Leg., Reg. Sess. (N.Y. 2015).

147. Joel Mathis, *Jersey May Mandate Cell Phone "Kill Switch,"* PHILA. MAG. (Sept. 22, 2014, 11:51 AM), http://www.phillymag.com/news/2014/09/22/jersey-may-mandate-cell-phone-kill-switch/.

148. Press Release, R. I. House of Representatives, Ruggerio Bill Calls for Smartphone Anti-Theft "Kill Switch," (Apr. 11, 2014), *available* at http://www.rilin.state.ri.us/pressrelease/_layouts/RIL.PressRelease.ListStructure/Forms/DisplayForm.aspx?List=c8baae31-3c10-431c-8dcd-9dbbe21ce3e9&ID=9676.

149. *See* Chokshi, *supra* note 5; Gutierrez, *supra* note 5.

150. Chokshi, *supra* note 5.

151. S. 1740, 88th Leg. (Minn. 2014).

152. *See id.*

153. *Id.*

154. *See id.*

155. Minn. Stat. § 325F.698 (2014).

location in the Minnesota Statutes openly indicates its purpose, as chapter 325F is titled "Consumer Protection; Products and Sales."[156] More narrowly, Section 698 is situated among others related to unauthorized cellular telephone use.[157]

Existing Minnesota law outlined in a preceding section, 325F.696, recognizes liability for individuals engaged in unauthorized cellular telephone use.[158] In that section, the Minnesota legislature defined unauthorized use as "use by a person other than the customer who does not have actual, implied, or apparent authority for the use."[159] Thus, Minnesota law already recognized liability for actions integral to smartphone theft, and sought to increase consumer protection with Section 698.[160]

A smart phone as defined in Section 698 is "a cellular phone or other device that: (1) is built on a smart phone operating system; (2) possesses advanced computing capability; (3) enables network connectivity; and (4) is capable of operating on a long-term evolution network and successor wireless data network communication standards."[161] Later in Section 698, specifically exclusions include many devices which could also be compatible with kill switch technology, such as tablets, laptop computers, and electronic readers.[162] By promulgating this working definition, the Minnesota Senate thereby limited the scope of Section 698 to target smartphones exclusively.[163]

Yet, the Minnesota Senate was noticeably succinct in drafting the kill switch subdivision of Section 698.[164] The subdivision reads, in its entirety, "[a]ny new smart phone manufactured on or after July 1, 2015, sold or purchased in Minnesota must be equipped with preloaded anti-theft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost."[165]

Smartphones are carefully defined in Section 698, subdivision 1. Anti-theft functionality, in contrast, is markedly ambiguous in Section 698, subdivision 2.[166] In fact, Section 698, Subdivision 2, never mentions a kill switch at all.[167] As a result, Section 698 as a whole is somewhat nebulous due to the lack of a definition, description, or other guidance indicating what constitutes anti-theft technology and how such technology would protect consumers.[168]

156. *Id.* § 325F.
157. *Id.*
158. *Id.* § 325F.696.
159. *See id.*
160. *See id.*; *id.* § 325F.698.
161. Minn. Stat. § 325F.698(1)(b).
162. *Id.*
163. *See id.*
164. *See id.* § 325F.698(2).
165. *Id.*
166. Hollister, *supra* note 95.
167. *See* Minn. Stat. § 325F.698(2); Molen, *supra* note 69.
168. Hollister, *supra* note 95.

Failure to even nominally set parameters regarding anti-theft technology will likely result in much uncertainty, and is perhaps the principal gaffe attributable to the Minnesota legislature in drafting Section 698.[169] Without further explanation, Section 698 may not give consumers, smartphone companies, or government officials enough direction to comply with or enforce the law. Consequently, Minnesotans may have to rely heavily on common law interpretations for Section 698 to be effectively implemented.

Ambiguity aside, Section 698 otherwise provides a seemly starting point for kill switch legislation in that it provides a working definition for smartphones and limits the scope of the mandate to such devices exclusively.[170] Section 698 necessitates all smartphones manufactured or sold in Minnesota have the capability of supporting anti-theft technological solutions, but does not explicitly require that solution be a kill switch.[171] Ultimately, Section 698 also does not require any smart phone come equipped with anti-theft technology or a kill switch at the point of sale.[172] Thus, the potential for consumers to opt-in and protect themselves at their own judgment is all Section 698 provides.[173]

California Senator Mark Leno has pointed out that many opt-in kill switches already exist in the private sector and many consumers fail to take advantage of such protections, rendering Minnesota's law as moot.[174] Nonetheless, Section 698 still increases consumer protection somewhat by making kill switch technology readily available to *all* smartphone users free of charge.[175]

Section 698 alone may only marginally decrease smartphone theft; yet it can still fortify public safety if compounded with other efforts. Correspondingly, Minnesota did not focus solely on protecting consumers by way of kill switch; that was only half of its legislative approach.[176] The other half of Minnesota's approach is largely independent from the success or failure of kill switch initiatives, and concentrates instead on undercutting the ability of criminals to discreetly convert stolen smartphones into cash.[177]

b. Disrupting the Smartphone Black Market Economy

In addition to mandating that all smartphones sold or manufactured in the state must have anti-theft capabilities, the Minnesota legislature enacted significant restrictions on the resale of smart phones.[178] These re-

169. Molen, *supra* note 69.
170. *See* Minn. Stat. § 325F.698(1)(b).
171. *See id.* § 325F.698(2).
172. *See* Chokshi, *supra* note 5.
173. *See* Minn. Stat. § 325F.698(2); Chokshi, *supra* note 5.
174. SECURE OUR SMARTPHONES, *supra* note 4, at ii.
175. Minn. Stat. § 325F.698(2).
176. *See id.*; Minn. Stat. § 325E.319; S.F. 1740, 88th Leg. (Minn. 2014).
177. *See* Minn. Stat. § 325E.319.
178. *See id.*

strictions were enacted in an effort to "protect[] consumers and crack[] down on secondary markets."[179] Article 2 of SF1740, titled "Resale of Cellphones," was renamed "Wireless Communications Devices; Acquisition for Resale," and codified as 325E.319 in the Minnesota Statutes ("Section 319").[180] By coupling anti-theft requirements in Section 698 with resale restrictions in Section 319, Minnesota formulated a more comprehensive approach than if it had propagated either section as a stand-alone act.

Situated in Chapter 325E regarding Trade Practices, Section 319 contains several restrictions on secondary market transactions and recognizes that kill switches only attack one dimension of the smartphone theft problem.[181] Section 319 specifically eliminates previously existing avenues criminals used to inconspicuously dispose of stolen devices in exchange for cash.[182] In this manner, Section 319 might encumber criminals by reducing the liquidity of stolen smartphones and obstructing the laundering of such devices through legitimate businesses.[183] The onus of these restrictions lies on wireless communications device dealers engaging in secondary market transactions, and, if violated, result in misdemeanor criminal penalties.[184]

i. Purchase or Acquisition Records

A key restriction in Section 319 is the requirement for smartphone dealers to catalog a variety of information, in writing, at the time of each transaction involving used communications devices.[185] Pursuant to Section 319, subdivision 2, smartphone dealers are required to record information including, but not limited to, the following:

> (1) An accurate account or description of the [smartphone] purchased or acquired; (2) the date, time, and place. . .the [smartphone] was purchased or acquired; (3) the name and address of the person selling or delivering the [smartphone]; (4) the number of the check or electronic transfer used to purchase the [smartphone]; (5) the number of the seller's driver's license, [or] Minnesota identification card number . . . ; (6) a statement signed by the seller, under penalty of perjury. . . attesting that the [smartphone] is not stolen . . . .[186]

To maximize the effectiveness and accessibility of such record keeping, subdivision 2 also contains a requirement that smartphone dealers

179. Press Release, U.S. Sen. Amy Klobuchar, With Cell Phone Thefts Surging, Klobuchar, Mikulski, Blumenthal, Hirono Introduce Legislation to Require a "Kill Switch" on Smartphones to Deter Thieves, Help Protect Consumers (Feb. 13, 2014).

180. *See* Minn. Stat. § 325E.319; S.F. 1740, 88th Leg. (Minn. 2014).

181. *See* Minn. Stat. § 325E.319.

182. *See id.* at subdiv. 6.

183. Marritz, *supra* note 35.

184. *See* Minn. Stat. § 325E.319 at subdiv. 7.

185. *See id.* at subdiv. 2.

186. *Id.*

are obligated to retain the records for three years.[187] Moreover, smartphone dealers must provide law enforcement access to records and devices at all times.[188]

To ensure accuracy and cooperation, subdivision 3 bars smartphone dealers from falsifying records, refusing to share records with law enforcement, or failing to maintain the records for three years.[189] Further restricting purchases or acquisitions from high-risk sellers, subdivision 3 also prohibits purchasing used devices from minors.[190]

Section 319, subdivisions 2 and 3, aim to increase the probability that criminals will be tracked down by law enforcement officials after pawning or selling stolen devices.[191] This, in turn, should deter criminals from selling stolen smartphones, which eliminates the incentive to steal in the first place. Regardless, Section 319, subdivisions 2 and 3, narrow some of the easiest avenues enjoyed by smartphone thieves to liquidate their bounty into cash.[192]

ii. Payment Methods

Further jeopardizing smartphone thieves' ability to maintain anonymity, Section 319, subdivision 4 eliminates cash as a legal method of payment for used smartphones.[193] Instead, "[a] wireless dealer shall pay for purchases of all used wireless communications by check mailed to a specific address or by electronic transfer."[194] By eliminating cash as an option for payment in transactions on the secondary smartphone market, Section 319 strategically forces criminals to either give up their addresses or risk being traced through electronic payment records.[195]

iii. Investigative Holds

Section 319, subdivision 5, forbids wireless communications device dealers from processing or selling devices that law enforcement officials have probable cause to believe are stolen, or are evidence of a crime, so long as law enforcement officials properly notify the wireless communications dealer in writing.[196] Additionally, law enforcement officials may confiscate devices that are confirmed to be stolen or evidence in a criminal case, subject to certain time constraints.[197] Consequently, the inclusion of Section 319, subdivision 5, may incentivize wireless communica-

187. *See id.*
188. *Id.*
189. *See id.* at subdiv. 3.
190. *Id.*
191. *See id.* at subdiv. 2–3.
192. *See id.*
193. *See id.* at subdiv. 4.
194. *Id.*
195. *See id.*
196. *See id.* at subdiv. 5.
197. *See id.*

tions device dealers to be more careful about the devices they purchase or acquire on the secondary market, so as not to lose property to seizure.

iv. Video Cameras

Pursuant to Section 319, subdivision 6, wireless communications device dealers are to invest in video cameras and ensure they are functional at all physical locations where business is conducted.[198] Video recorded by such cameras must be shown to law enforcement officials upon request, and wireless communications device dealers must retain the video recordings for a minimum of thirty days.[199] This surveillance mechanism will allow law enforcement to identify persons associated with peddling stolen smart phones by a physical description, thereby facilitating efforts of bringing them into custody and prosecuting them for their crimes.

2. California's Kill Switch Law

California's kill switch law, the second to be passed nationwide, originated as Senate Bill 962 in the California Senate.[200] California Governor Jerry Brown approved Senate Bill 962 on August 25, 2014, which was codified in Chapter 275, Section 22761 of the California Business and Professions Code ("Section 22761").[201] The enactment of Section 22761 is of great magnitude from a national and global perspective, in part, because California is an especially influential state economically and politically. California has the largest state population in the United States by a long shot,[202] and correspondingly touts the most members in the House of Representatives.[203] California is also home to the nation's largest economy, an economy so large that in the past several years it passed the Italian, Russian, and Brazilian economies to become the seventh largest on Earth.[204] Due to the large size of California's population and economy, there are a correspondingly high number of lawmakers, smartphone users, manufacturers, and wireless carriers with California ties.

a. Characteristics of Section 22761

California's kill switch law has some similarities with Minnesota's law, but also many characteristics unique to Section 22761. According to

198. *See id.* at subdiv. 6.

199. *Id.*

200. *See* An Act to Add Section 22761 to the Business and Professions Code, Relating to Mobile Communications Devices, S. 962, 2014 Leg. (Cal. 2014) (enacted).

201. *See id.*; 275 CAL. BUS. & PROF. CODE § 22761 (2014).

202. *Population Estimates*, U. S. CENSUS BUREAU (July 1, 2014), http://www.census.gov/quickfacts/table/PST045214/06,00.

203. *Seats in the House of Representatives (Most Recent) by State*, STATEMASTER, http://www.statemaster.com/graph/gov_sea_in_the_hou_of_rep-government-seats-house-representatives (last visited Sept. 7, 2015).

204. Michael B. Marois & Shin Pei, *California Economy Surpasses Brazil's*, SBS (Jan. 18, 2015, 3:31 PM), http://www.sbs.com.au/news/article/2015/01/18/california-economy-surpasses-brazils.

the language of Section 22761, kill switches "when enabled, [should] be able to withstand a hard reset . . . and prevent reactivation of the smartphone on a wireless network *except by an authorized user*."[205] Thus, California's kill switch law is of the soft variety, akin to Minnesota's, because a smartphone may be reactivated if an authorized user recovers their device.[206]

Section 22761 also requires all smartphones sold in the state to have kill switch technology installed and activated as a *default setting* at the time of sale.[207] Under this provision, retailers who sell a smartphone without a kill switch will be fined between $500 and $2,500.[208] Thus, Section 22761 is of the opt-out variety—divergent from Minnesota's opt-in version.[209] Based on a numbers game theory regarding opt-in versus opt-out laws, Section 22761 is likely to have a greater deterrent effect on thieves than Minnesota's analog.[210] The theory is evidenced in the marketplace; where some smartphone carriers and manufacturers already offer kill switch technology on an opt-in basis, yet many consumers fail to take advantage of the security option.[211]

> By having it opt-out rather than opt-in, law enforcement believes many more people will leave it switched on and so the chance that any given smartphone will be protected will be much higher. The deterrent aspect of the kill switch relies on this numbers game: If a phone is likely to have the software, thieves have less incentive to steal it. If it likely doesn't, the chance it will be stolen goes up.[212]

Section 22761 is likely to have a greater deterrent effect on thieves, and deterrence indeed a primary objective of kill switch legislation,[213] yet California's scheme is far from perfect. Among the most problematic aspects of Section 22761 is that it creates a process for government officials to access and activate kill switches, disabling the smartphones of private individuals. This intrusive option is not seen in Minnesota's kill switch law, and it could lead to the government infringing on individuals' civil liberties.[214]

205. *See* Molen, *supra* note 69.
206. *See id.*
207. *See* Gutierrez, *supra* note 5.
208. Gerry Smith, *States Pass Smartphone 'Kill Switch' Bills That Wireless Companies Hate*, HUFF. POST (May 8, 2014, 4:46 PM), http://www.huffingtonpost.com/2014/05/08/smartphone-kill-switch_n_5290107.html.
209. *See* SECURE OUR SMARTPHONES, *supra* note 4, at i; *see also* Chokshi, *supra* note 5; Gutierrez, *supra* note 5; Molen, *supra* note 69.
210. Martyn Williams, *10 Things to Know About the Smartphone Kill Switch*, PCWORLD, (June 24, 2014, 3:28 PM), http://www.pcworld.com/article/2367480/10-things-to-know-about-the-smartphone-kill-switch.html.
211. *See* SECURE OUR SMARTPHONES, *supra* note 4.
212. Williams, *supra* note 210.
213. *See* Molen, *supra* note 69.
214. *See infra* Part III.A.2.b.ii.

b. Constitutional Considerations

Statutory language included in Section 22671 allows government agencies to shut down smartphone communications using the kill switch.[215] That provision, included in the name of public safety, might instead be used to infringe on civil liberties.[216] Thus, it is important to consider the constitutional basis for Section 22671 and address constitutional issues that may arise from its enactment.

i. California's Kill Switch Law has Basis in the Police Power

Indeed, preserving the safety of the public is an important if not essential government function.[217] According to widespread judicial interpretation, the Tenth Amendment provides the states with the police power, or "the power to regulate for the benefit of public health, safety, morals, or general welfare except as restrained by the U.S. Constitution."[218] As apparent in the stated purpose of Section 22761, the focus of the law is to reduce smartphone theft and promote safety.[219] Thus, Section 22761 has some constitutional basis in the Tenth Amendment.[220] Insofar that it serves to increase health and safety and promote the general welfare by confronting the smartphone theft epidemic, Section 22761 is in line with the police power.[221]

In its exercise of the police power and drafting Section 22761, California was careful to avoid preemption and unconstitutionality in the text of the law.[222] Precautionary measures taken by California in this regard include, but are not limited to: avoiding state and federal due process violations by clearly stating what is required by the law for manufacturers and retailers to avoid penalties, avoiding outright violations of the First[223] and Fourth[224] Amendments by taking steps to protect civil liberties and privacy, and avoiding express preemption by deleting provisions di-

215. *See* 275 CAL. BUS. & PROF. CODE § 22761(B)(4)(e) (2014).

216. Jake Laperruque, *California "Kill Switch" Bill Could Be Used to Disrupt Protests*, CTR. FOR DEMOCRACY & TECH. (Aug. 15, 2014), https://cdt.org/blog/california-kill-switch-bill-could-be-used-to-disrupt-protests/.

217. JOEL B. PLANT & MICHAEL S. SCOTT, EFFECTIVE POLICING AND CRIME PREVENTION 6 (2009).

218. 1 JOHN J. DELANEY ET AL., HANDLING THE LAND USE CASE: LAND USE LAW, PRACTICE & FORMS § 2:3 (3d ed.).

219. *Hearing on S.B. 962 Before the S. Comm. On Energy, Utils., & Commc'ns.,* 2014 Leg., 2013–2014 Sess. 3 (Cal. 2014).

220. *See* U.S. CONST. amend. X.

221. *See id.*; DELANEY ET AL., *supra* note 218.

222. *See* U.S. CONST. amend. IV*;* S.B. 962, 2013–14 Leg. (Cal. 2014); *Hearing on S.B. 962 Before the S. Comm. On Energy, Utils., & Commc'ns.,* 2014 Leg., 2013–2014 Sess. (Cal. 2014).

223. U.S. CONST. amend. I.

224. U.S. CONST. amend. IV.

rectly in opposition with existing federal statutes.[225] Thus, it is highly likely Section 22761 would survive judicial review[226] if eventually challenged.

ii. California's Kill Switch Law Poses a Threat to Civil Liberties

Even if California's kill switch law has a textual basis in the police power, civil liberties violations may nonetheless arise when the law is implemented in practice.[227] Parties who opposed Section 22761 before it was even enacted posited that First Amendment[228] violations, among other complications, might ensue if the law was enacted.[229] For example, the Center for Democracy & Technology ("CDT"),[230] which harbors serious concerns about government kill switch mandates in general, stated that pursuing Section 22761 could result in a variety of security and privacy problems.[231]

CDT points to a specific provision of the California kill switch law, Section 22761(B)(4)(e),[232] which allows police or other government officials to activate kill switches, so long as doing so conforms to guidelines set out in Section 7908 of the California Public Utilities Code.[233] This provision leaves the door open to potential abuses such as government agents suppressing protests and other exercises of speech, as "[p]olice could use the kill switch to shut down all phones in a situation they unilaterally perceive as presenting an imminent risk of danger."[234]

In essence, California's kill switch law arms government officials with the technical capabilities to shut down smartphones statewide.[235] While compliance with Section 7908 of the California Public Utilities Code will require government officials to obtain a court order to engage in shutting down smartphones via kill switch, a new and generously invasive legal process for government interference is nonetheless created.[236] Additionally, the California Public Utilities Code is not binding on law enforcement officials outside California, creating significant risk for

225. *See Hearing on S.B. 962 Before the S. Comm. On Energy, Utils. & Commc'ns.,* 2014 Leg., 2013–2014 Sess. 3–6 (Cal. 2014).

226. *See* Marbury v. Madison, 5 U.S. 137 (1803).

227. Nocandro Iannacci, *Lawmakers Call for a Smartphone 'Kill Switch'*, PHILLY.COM, http://www.philly.com/philly/business/Lawmakers_call_for_a_smartphone_kill_switch.html?c=r (last updated Aug. 27, 2014).

228. U.S. CONST. amend. I.

229. Iannacci, *supra* note 227.

230. *See* Jake Laperruque, *"Kill Switch" Legislation Are Essentially Unnecessary Government Mandates*, CTR. FOR DEMOCRACY & TECH. (Mar. 04, 2014), https://cdt.org/blog/kill-switch-legislation-are-essentially-unnecessary-government-mandates/.

231. *See* Iannacci, *supra* note 227.

232. 275 CAL. BUS. & PROF. CODE § 22761(B)(4)(e) (2014).

233. *See* Laperruque, *supra* note 216.

234. *Id.*

235. *See* Kim Zetter, *How Cops and Hackers Could Abuse California's New Phone Kill-Switch Law*, WIRED (Aug. 26, 2014, 5:44 PM), http://www.wired.com/2014/08/how-cops-and-hackers-could-abuse-californias-new-phone-kill-switch-law/.

236. *Id.*

abuse of the kill switch by officials elsewhere.[237] Thus Section 22761 is embedded with statutory language that alarmingly increases police power at the expense of civil liberties.[238]

Indeed, California officials have already exhibited a propensity to suppress public demonstrations by closing lines of communication, an authoritarian method that will become easier and possibly more commonplace once all smartphones are equipped with kill switch technology.[239] In one instance, on August 11, 2011, officials at the Bay Area Rapid Transit System (BART) in San Francisco interrupted cellular and WiFi service to frustrate the ability of people to organize and protest a fatal police shooting.[240] In describing the BART scenario, an ACLU attorney aptly stated, "[a]ll over the world, people are using mobile devices to protest oppressive regimes, and governments are shutting down cell phone towers and the Internet to top them . . . It's outrageous that in San Francisco, BART is doing the same thing."[241]

In the wake of clashes between police and civilians, such as the events that transpired in Ferguson, Missouri during August 2014, the risk of abuse is especially apparent.[242] Ridden with what were likely civil liberties violations, police conduct during the Ferguson protests included that of arresting media personnel, threatening protesters, and using semi-automatic weapons, tear gas, and rubber bullets to suppress the demonstrations.[243] According to Jake Laperruque of CDT, "[i]f the California bill were in place in Missouri, these officers might [have] deploy[ed] the government kill switch . . . using the mandated technology to stop coordination between protesters, cut off access to outside information, and shut down video recordings that can deter police conduct."[244] Therefore, because Section 22761(B)(4)(e) creates a legal process for government officials to shut down individuals' smartphones, California's kill switch law poses a threat to civil liberties.

237. *Id.*

238. *See* 275 CAL. BUS. & PROF. CODE § 22761(B)(4)(e) (2014) ("Any request by a government agency to interrupt communications service utilizing a technological solution required by this section is subject to Section 7908 of the Public Utilities Code.").

239. *See* Erika J. Pitzel, *Bay Area Rapid Transit Actions of August 11, 2011: How Emerging Digital Technologies Intersect With First Amendment Rights*, 29 GA. ST. U. L. REV. 783 (2013); Laperruque, *supra* note 216.

240. *See* Pitzel, *supra* note 239, at 785–87; Laperruque, *supra* note 216.

241. Jennifer Abel, *California Kill-Switch Bill Worries Civil Liberty Advocates*, CONSUMER AFFAIRS (Aug. 27, 2014), http://www.consumeraffairs.com/news/california-kill-switch-bill-worries-civil-liberty-advocates-082714.html.

242. Laperruque, *supra* note 216.

243. *See id.*

244. *See id.*

B. Public Policy, Regulation, and Innovation in the Smartphone Industry

As a matter of policy, reducing the issue of smartphone theft to one that must be solved through kill switch legislation is unpopular in some camps.[245] Policymakers and smartphone industry leaders in opposition to the Minnesota and California kill switch laws, and kill switch legislation in general, argue that such legislation unduly burdens the smartphone industry and could stifle innovation.[246] Yet, as demonstrated by regulation in other major U.S. industries, regulation can benefit the public by protecting health and safety.[247] The question is whether kill switch legislation, with all of its potential benefits, can be implemented without unduly encumbering the smartphone industry or stifling innovation.

1. The Smartphone Industry Opposes Kill Switch Laws

Many major players in the smartphone industry oppose kill switch laws.[248] These firms maintain that despite well-founded legislative intent, kill switch laws are unnecessary due to existing and forthcoming private sector solutions.[249] Across the board, smartphone industry members who oppose kill switch legislation also echo the same basic argument: "[T]echnology is fast; the law is slow . . . institutionalizing specific technical solutions—such as making every cell phone manufacturer feature a 'kill switch' program—is risky."[250]

For example, a coalition of technology and business industry leaders including, but not limited to, Microsoft, Sprint, AT&T, Verizon, T-Mobile, Motorola, Google, and the California Chamber of Commerce argued fervently against California's kill switch law.[251] According to the coalition, the law is impractical.[252] In a letter to California Senator Mark Leno, the coalition proclaimed: "[W]hat state lawmakers mandate as a solution today may not be the solution consumers demand or need tomorrow."[253]

245. *See* Adi Kamdar, *EFF Opposes California's Cell Phone "Kill Switch" Bill,* ELEC. FRONTIER FOUND. (June 18, 2014), https://www.eff.org/deeplinks/2014/06/eff-opposes-californias-cell-phone-kill-switch-bill.

246. *See* CAL. S. RULES COMM. 2013-2014, ANALYSIS OF SB 962 ON AUG. 8, 2014, at 8 (2014) [hereinafter CALIFORNIA SB 962 ANALYSIS]; Kamdar, *supra* note 245.

247. *See, e.g.*, *History of Mine Safety and Health Legislation*, U.S. DEPT. OF LABOR, http://www.msha.gov/MSHAINFO/MSHAINF2.HTM (last visited Sept. 8, 2015); *Safety and Health Add Value*, U.S. DEPT. OF LABOR, https://www.osha.gov/Publications/safety-health-addvalue.html (last visited Sept. 8, 2015).

248. *See* CALIFORNIA SB 962 ANALYSIS, *supra* note 246, at 8.

249. *See id.*

250. Kamdar, *supra* note 245.

251. Microsoft Letter, *supra* note 111.

252. *Id.*

253. *Id.*

2. Will Kill Switch Laws Stifle Innovation in the Smartphone Industry?

Though the smartphone industry claims kill switch laws will stifle innovation, the effects of regulation on other industries does not wholly substantiate this claim.[254] Regulation is "the implementation of rules by public authorities and governmental bodies to influence market activity and the behavior of private actors in the economy."[255] Technological innovation, often confused with invention, is defined as "the first commercially successful application of a new technical idea."[256] Despite common discourse in the smartphone industry that innovation is negatively affected by regulation,[257] the effects of regulation on innovation are more nuanced. Indeed, innovation and regulation are umbrella terms, and there are numerous types and classifications of each.[258] The outcomes of interactions between the various types are fact specific, and fluctuate depending on specific companies, time horizons, and sectors of the economy.[259]

Scholars have studied the varied effects of regulation on innovation extensively.[260] The purpose of this Part of the Note is not to explore that large body of work in great detail; rather, it is to focus on the relationship between kill switch laws and innovation in the smartphone industry. In examining that relationship, this Part of the Note reviews the types of regulation, innovation, and related market forces relevant to kill switch law analysis.

a. Social Regulation

Social regulation is "the imposition of requirements on firms to protect the welfare of society or the environment."[261] Thus, kill switch laws, which impose kill switch requirements on smartphone companies to protect users, are a form of social regulation. Historically, social regulation has been used as a tool to correct market externalities.[262] Social regulation has effectively corrected externalities stemming from U.S. industries

254. *See* Knut Blind, *The Impact of Regulation on Innovation* 6 (Nesta Working Paper No. 12/02, 2012), *available at* https://www.nesta.org.uk/sites/default/files/the_impact_of_regulation_on_innovation.pdf.

255. *Id.*

256. Kathleen M. Rest & Nicholas A. Ashford, *Regulation and Technological Options: The Case of Occupational Exposure to Formaldehyde*, 1 HARV. J. L. & TECH. 63, 63 n.1 (1988).

257. *See* Microsoft Letter, *supra* note 111.

258. Blind, *supra* note 254, at 2–4.

259. *Id.* at 2.

260. *See, e.g.*, David E. Adelman & Kirsten H. Engel, *Reorienting State Climate Change Policies to Induce Technological Change*, 50 ARIZ. L. REV. 835 (2008); Stuart Minor Benjamin & Arti K. Rai, *Fixing Innovation Policy: A Structural Perspective*, 77 GEO. WASH. L. REV. 1 (2008); Timothy F. Malloy & Peter Sinsheimer, *Innovation, Regulation and the Selection Environment*, 57 RUTGERS L. REV. 183 (2004); Rest & Ashford, *supra* note 256; Konstantinos K. Stylianou, *An Innovation-Centric Approach of Telecommunications Infrastructure Regulation*, 16 VA. J.L. & TECH. 221 (2011); Blind, *supra* note 254.

261. LUKE A. STEWART, THE IMPACT OF REGULATION ON INNOVATION IN THE UNITED STATES: A CROSS-INDUSTRY LITERATURE REVIEW 7 (2010), *available at* http://www.itif.org/files/2011-impact-regulation-innovation.pdf.

262. *Id.*

including, but not limited to, the automobile, chemical, energy, and pharmaceutical industries.[263] For example, compliance laws promulgated by the Environmental Protection Agency[264]—social regulations—have reduced air pollution from manufacturing plants—market externalities.[265]

Crime, though subtler than pollution, has been found to be a negative externality of economic growth.[266] The rise of smartphone technology, which fortified "the wireless industry [as] one of the most important and vibrant sectors of our economy[,]"[267] evidently has produced crime as a negative externality.[268] In response, kill switch laws—social regulations— aim to reduce smartphone theft and violent crime—market externalities.

b. Effects of Social Regulation on Innovation

The effect of social regulation on innovation is multi-directional.[269] Ultimately, whether kill switch regulations stimulate or stifle innovation in the smartphone industry depends on whether the positive effects of regulation outweigh the negative effects.

i. Compliance Burdens Stifle Innovation in the Short Term

Social regulation can have a negative effect on innovation by imposing compliance burdens on firms.[270] Compliance burdens result when a new law requires a firm to reallocate resources—time, money, expertise, personnel, etc.—away from innovative projects and towards compliance efforts.[271] These costs are most relevant in the short term.[272] Insofar as compliance burdens are not so high that firms must cease to operate, such burdens can later be counteracted, at least to some degree, by positive effects of social regulation on innovation.[273]

ii. The Mixed Effects of Policy Uncertainty

Social regulation is typically preceded by uncertainty that has mixed effects on innovation. Policy uncertainty materializes whenever individual firms or industries expect regulation to be enacted at a future time.[274] In anticipation of new laws, firms may preemptively begin innovating

263. *Id.* at 1, 22.
264. *See, e.g.*, U. S. ENVTL. PROT. AGENCY, http://www.epa.gov/ (last visited Sept. 8, 2015).
265. STEWART, *supra* note 261, at 7.
266. David D. Hemley & Lee R. McPheters, *Crime as an Externality of Economic Growth: An Empirical Analysis*, 19 AM. ECON. 45, 45–46 (1975).
267. Microsoft Letter, *supra* note 111.
268. Williams, *supra* note 4.
269. Blind, *supra* note 254, at 25.
270. STEWART, *supra* note 261, at 2.
271. *Id.*
272. *Id.*
273. *Id.*
274. *Id.* at 3–4.

their products and practices to achieve compliance.[275] Conversely, however, firms may divert resources away from other innovative projects, thereby decreasing innovation.[276] Yet, a third possibility occurs when there is a high degree of policy uncertainty, and the optimal business decision is contingent on whether new laws will be enacted. In these situations, firms will simply stop investing in innovative projects altogether, awaiting the outcome of a given bill.[277]

Policy uncertainty has resulted in mixed results with regard to kill switch laws. In anticipation of the Minnesota and California smartphone laws, most major smartphone companies joined the kill switch initiative.[278] Inasmuch as they diverted resources from other innovative projects to comply, these firms suffered compliance costs.[279] Yet in the same vein, insofar as the Minnesota and California kill switch bills encouraged firms to develop products they may not have otherwise pursued, policy uncertainty spurred innovation.[280]

iii. Social Regulation Stimulates Innovation in the Long Run

According to Knut Blind,[281] professor of standardization at the Erasmus University of Rotterdam,[282] and professor of innovation economics at the Technical University of Berlin,[283] social regulation tends to encourage innovation, rather than stifle it.[284] Despite initial compliance costs having a negative effect on innovation, social regulation can produce incentives and spillover benefits from compliance that result in increased innovative activities in the long run.[285]

Consider compliance innovation, which occurs when, in response to a new law, non-compliant firms develop their products and practices in order to comply.[286] Indeed, for smartphone companies that have not yet developed kill switch technology, kill switch laws force them to innovate in this area immediately.[287] Kill switch laws also stimulate innovation in firms that have already developed kill switches.[288] Although such firms are technically capable of providing kill switches to users, their processes for large-scale manufacturing or distribution may be inefficient and cost-

275. *Id.* at 4.
276. *Id.*
277. *Id.*
278. *See* Chokshi, *supra* note 5.
279. *See* discussion *infra* Part III.B.2.b.iii.
280. *See* discussion *infra* Part III.B.2.b.iii.
281. *Prof. Knut Blind*, ROTTERDAM SCH. OF MGMT., ERASMUS UNIV., http://www.rsm.nl/ people/knut-blind/ (last visited Sept. 8, 2015).
282. *Id.*
283. *Id.*
284. Blind, *supra* note 254, at 16.
285. *Id.* at 25.
286. STEWART, *supra* note 261, at 2.
287. *See id.*
288. *See id.*

ly.[289] Consequently, these firms will seek innovative process changes to reduce their cost of complying.[290]

Social regulation can also positively effect innovation by expanding market reach or even generating entirely new markets.[291] This phenomenon occurs when a social regulation creates innovation incentives by "increas[ing] the acceptance of new products among consumers and promotes their diffusion."[292] Accordingly, kill switch laws, once in effect, promptly increase the number of kill switch users.[293] This sudden growth in the number of kill switch users creates a new demographic for firms to target.[294] Presumably, kill switch quality differences across manufacturers and carriers could eventually factor into consumers' purchasing decisions—similar to consumers considering vehicle safety ratings when purchasing an automobile.[295] As users must decide which of the many kill switch options to choose, developers must compete for users and market share.[296] Therefore, kill switch laws produce an additional demographic of users that could fuel competition and incentivize innovation of more useful and effective anti-theft solutions.[297]

The Minnesota and California kill switch laws thus raise the baseline for smartphone anti-theft technology. As kill switches become the norm, smartphone developers and manufacturers can enter a second stage of innovation. This stage will offer the opportunity to both refine their kill switches and to explore other advanced security options. Likewise, they can continue to pursue innovation projects unrelated to smartphone theft.

This second stage of innovation, after the initial kill switch development stage, reflects differing short term and long term effects of social regulation. Due to initial compliance costs placing a burden on firms, innovation is negatively effected over the short term.[298] Yet over the long term, other innovation—stemming from that same original duty to comply with social regulation—will generally outweigh initial compliance costs.[299] Ultimately, by encouraging or even forcing firms to make technical changes, social regulation accelerates the adoption of new processes

289. *See id.*

290. Timothy F. Malloy, *Regulating by Incentives: Myths, Models, and Micromarkets*, 80 TEX. L. REV. 531, 546 (2002).

291. Blind, *supra* note 254, at 25.

292. *Id.* at 19.

293. *See id.*

294. *See id.*

295. *10 Safety Checks to Make Before You Buy*, CONSUMER REPORTS, http://www.consumerreports.org/cro/2012/12/10-safety-checks-to-make-before-you-buy/index.htm (last updated Feb. 2014).

296. *See* Michael E. Porter & James E. Heppelmann, *How Smart, Connected Products Are Transforming Competition*, HARV. BUS. REV. (Nov. 2014), https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition ("In any industry, competition is driven by five competitive forces: the bargaining power of buyers, the nature and intensity of the rivalry among existing competitors, the threat of new entrants, the threat of substitute products or services, and the bargaining power of suppliers.").

297. *See id.*

298. *See* discussion *supra* Part III.B.2.b.i.

299. *See* discussion *supra* Part III.B.2.b.i.

and products, and "generat[es] additional incentives for innovative activities."[300]

C. Smartphone Anti-theft Bills at the Federal Level

In addition to various states pursuing kill switch legislation, multiple bills have been introduced at the federal level designed to combat the smartphone theft epidemic. Federal legislation may be advantageous inasmuch as it could increase consistency across the states and cover the maximum number of smartphone users possible.

1. The Smartphone Theft Prevention Act

On February 13, 2014, Senator Amy Klobuchar of Minnesota introduced Senate Bill 2032,[301] the Smartphone Theft Prevention Act, in the U. S. Senate.[302] The bill was co-sponsored by Senator Barbara Mikulski of Maryland, Senator Mazie Hirono of Hawaii, and Senator Richard Blumenthal of Connecticut.[303] New York Representative Jose Serrano introduced a companion bill, House Bill 4065,[304] in the U.S. House of Representatives on the following day.[305] The Smartphone Theft Prevention Act is an important step towards the federal government recognizing and combatting the smartphone theft epidemic.[306]

The bill, closely mirroring the California kill switch law, calls for an opt-out variety of kill switch.[307] Opt-out kill switch laws, as discussed previously in this Note, likely have a greater deterrent effect than opt-in laws.[308] Despite mirroring the California kill switch law, the Smartphone Theft Prevention Act excludes problematic statutory language in California's kill switch law[309] that leaves the door open for government abuses and infringement on civil liberties.[310]

The Smartphone Theft Prevention Act poses multiple advantages.[311] If enacted, it could eliminate compliance issues smartphone companies might face with state-by-state laws, namely by offering offer one national

300. Blind, *supra* note 254, at 1.

301. S. 2032, 113th Cong., 2d Session (2014).

302. Martyn Williams, *Federal Smartphone Kill-Switch Legislation Proposed*, PCWORLD (Feb. 13, 2014, 12:16 AM), http://www.pcworld.com/article/2097840/federal-smartphone-killswitch-legislation-proposed.html.

303. *Id.*

304. H.R. 4065, 113th Cong., 2d Session (2014).

305. Martyn Williams, *Second Federal 'Kill-Switch' Bill Introduced Targeting Smartphone Theft*, PCWORLD (Mar. 3, 2014, 10:58 AM), http://www.pcworld.com/article/2103820/second-federal-kill switch-bill-introduced-targeting-smartphone-theft.html.

306. *See* S. 2032.

307. *See* Molen, *supra* note 69.

308. *See supra* Part III.A.2.

309. *See* Laperruque, *supra* note 216.

310. *See* S. 2032; H.R. 4065, 113th Cong., 2d Session (2014).

311. *See supra* Part IV.B.2.b (describing advantages of opt-out characteristics of California's kill switch law mirrored by the Smartphone Theft Prevention Act).

standard.[312] Also, a federal kill switch law would offer protection to consumers in states where legislatures have not pursued kill switch legislation.

In addition, the Smartphone Theft Prevention Act offers a significantly higher level of consumer protection as compared to existing state laws.[313] The federal government has sovereign power to control imports[314] and extradite criminals from foreign nations.[315] This formidable aspect of a federal kill switch law is especially important in combatting the global smartphone black market, which transcends state and national borders.[316] Thus, by providing sounder oversight on foreign manufacturers and stronger enforcement on criminals evading justice by fleeing the country, the Smartphone Theft Prevention Act could successfully enhance consumer protection.[317]

2. The Mobile Device Theft Deterrent Act of 2013

Much as Minnesota's legislative approach couples kill switch requirements with legislation aimed at disrupting the smartphone black market economy, the Mobile Device Theft Deterrent Act[318] is a bill that, if coupled with the Smartphone Theft Prevention Act, would result in more comprehensive consumer protection.[319] New York Senator Charles Schumer introduced the bill in the U.S. Senate in May 2013 "as part of an ongoing effort to crack down on the black market for stolen [smart] phones."[320]

This federal bill is not a kill switch bill at all, but instead disrupts the smartphone black market economy by increasing the severity of criminal penalties on individuals caught tampering with mobile device identification numbers.[321] The identification numbers, known as International Mobile Equipment Identity (IMEI) numbers,[322] are assigned to smartphones for cataloging purposes in the United States device registry, a database that keeps track of stolen smartphones.[323] If enacted, the Mobile Device Theft Deterrent Act will provide criminal punishment of up to five years in prison for those convicted of tampering with IMEIs.[324]

At first glance the proposal seems harsh, but according to Senator Schumer, "we must make it clear that if you alter a cell phone identifica-

312. *See* Molen, *supra* note 69.
313. *See* U.S. CONST. art. I, § 10; *Id.* at art. II, § 2; 18 U.S.C. § 3184 (2012).
314. U.S. CONST. art. I, § 10.
315. *See id.* at art. II, § 2; 18 U.S.C. § 3184.
316. *See* discussion *supra* Part III.C.1.
317. *See* U.S. CONST. art. II, § 2; 18 U.S.C. § 3184.
318. S. 1070, 113th Cong. (2013).
319. *See* Damon Poeter, *Schumer Introduces Bill to Make Cell Phone ID Tampering a Crime*, PCMAG (May 24, 2013, 2:03 PM), http://www.pcmag.com/article2/0,2817,2419491,00.asp.
320. *Id.*
321. *Id.*
322. *Id.*
323. *Id.*
324. *Id.*

tion number of a stolen phone, you will face serious consequences."[325] Thus, the Mobile Device Theft Deterrent Act may discourage criminals from stealing smartphones and then avoiding detection on the United States device registry by tampering with the stolen phone's IMEI.

IV. RECOMMENDATION

Hold on to your smartphones! Even as you read this Part of the Note, it is probable that every eleven seconds a consumer in the United States will fall victim to smartphone theft.[326] Based on the analysis in this Note, kill switch legislation offers a viable option in combatting the smartphone theft epidemic and should be pursued.[327] The legislative approaches taken by Minnesota and California illuminate central issues in formulating a methodology to reduce smartphone theft.[328] To achieve maximum consumer protection for smartphone users, this Part of the Note recommends kill switch legislation should be pursued, and specifically, that Congress enact a federal smartphone kill switch law, featuring a blend of the Minnesota and California approaches.

A. Kill Switch Legislation Should Be Pursued

The ominous reality of rampant smartphone theft, often violent, is incontrovertible.[329] Despite emerging kill switch technology in the private sector,[330] the simple fact remains that many smartphone users have yet to equip their device with a kill switch.[331] For some, this is due to the technical incapability of their device to support a kill switch.[332] For many, this is due to a personal failure to opt-in to available kill switch technology, resulting from lack of knowledge, naiveté, or some combination of the two.[333] In either case, legislation can provide more users the protection offered by kill switch technology, and increase the deterrent effect on smartphone thieves.[334]

Based on the analysis in this Note, kill switch legislation does not unduly burden the smartphone industry or stifle innovation.[335] Adversaries of kill switch laws, especially lawmakers aligning themselves with the smartphone industry, must reconsider their blanket assumptions regarding the effect of kill switch laws on innovation. As previously discussed in this Note, kill switch laws, like other forms of social regulation,

325. *Id.*
326. *See* Tapellini, *supra* note 4 (According to simple arithmetic, if there are 31,536,000 seconds and 3,100,000 smartphone thefts in a year, a smartphone theft will occur every 10.17 seconds.).
327. *See* discussion *supra* Part III.
328. *See* discussion *supra* Part III.A.
329. *See* Smith, *supra* note 30; Williams, *supra* note 4.
330. *See* discussion *supra* Part II.3.b.
331. SECURE OUR SMARTPHONES, *supra* note 4.
332. *Id.*
333. *Id.*
334. *See id.*
335. *See* discussion *supra* Part III.B.

will likely have a positive effect on innovation in the long run.[336] Also, given that most major smartphone companies have already developed basic kill switch capabilities independently, initial compliance costs will be manageable, and innovation will not be stifled significantly in the short term.[337]

Candidly, even if a slight burden is placed on firms in the smartphone industry, it is outweighed by the benefit society will derive from kill switch legislation. If mandatory kill switch legislation is enacted, consumers stand to save over $2 billion annually in smartphone replacement and insurance costs, and will gain the inherent value of less crime and increasing safety for users.[338] To avoid kill switch legislation disproportionately favors a handful of smartphone firms, especially those reaping the benefits of selling replacement devices and premium insurance packages, at the expense of millions of individual consumers. Therefore, kill switch legislation is in the best interest of society and should be pursued.

B. A Model Legislative Approach

The effectiveness of kill switch legislation is contingent on its specific characteristics and provisions. Based on the analysis in this Note, the optimal legislative approach is a federal kill switch law containing provisions from both the Minnesota and California kill switch laws.[339]

1. A Federal Kill Switch Law Should be Enacted

An optimal approach legislative approach must feature a federal kill switch law. Though enacting kill switch laws on a state-by-state basis may benefit some consumers, this approach, as evidenced by existing kill switch laws and bills, results in uneven coverage and inconsistent standards across the fifty states. Consequently, smartphone users residing states without kill switch laws might be subject to a higher risk of theft than those in states with kill switch laws. In addition, varied standards promulgated by different state legislatures will make it more difficult for companies to comply. Lastly, and perhaps most importantly, the clout of the federal government is necessary to properly enforce an ideal kill switch law.[340] To effectively disrupt the smartphone black market, which transcends state and national borders, the federal powers over importation and extradition are essential.[341] Therefore, a federal kill switch law should be enacted.

336. *See* discussion *supra* Part III.B.2.b.ii.
337. *See* discussion *supra* Part III.B.2.b.i.
338. *See* DUCKWORTH, *supra* note 12, at 1–3.
339. *See* discussion *supra* Part III.
340. *See* discussion *supra* Part III.C.
341. *See* discussion *supra* Part III.C.

2. Specific Provisions of an Ideal Kill Switch Law

The kill switch laws enacted by Minnesota and California are commendable yet imperfect attempts at solving the smartphone theft epidemic. Each, however, offers Congress guidance on what specific provisions should be included—and excluded—when formulating a refined, comprehensive federal kill switch law.

a. Takeaways from Minnesota's Legislative Approach

Minnesota's opt-in approach, merely mandating that all smartphones be capable of being equipped with a kill switch, is likely to change the status quo only slightly.[342] Though some users cannot equip their devices with a kill switch due to technical incapability, most users' devices are not equipped because they negligently fail to opt-in.[343] Thus, Minnesota's opt-in approach has a weaker deterrent effect than California's opt-out approach: thieves will nonetheless steal smartphones capable of supporting kill switch technology, in the hopes the devices are not equipped or engaged with a kill switch.[344]

The true strength of Minnesota's kill switch law is that it recognizes the smartphone theft epidemic is "a monolithic problem that can be solved by a single killer app."[345] Similar to Minnesota's approach, Congress should supplement any kill switch requirement with provisions specifically aimed at disrupting the smartphone black market.

In this regard, an ideal federal kill switch law should require all smartphone retailers to keep detailed purchase and acquisition records, and should eliminate cash as a legal payment method for all transactions involving smartphones on the secondary market. Also, if law enforcement has probable cause to believe a smartphone is stolen, and notifies the wireless communication devices dealer in possession of the smartphone of that belief, the wireless communication devices dealer should be barred from selling or otherwise disposing of the device in question.

Congress should also include additional measures, such as requiring wireless communication devices dealers to furnish the premises of any place of business with video cameras. In essence, any measure that hinders the ability of thieves to anonymously convert stolen phones into cash deserves consideration.

In order to ensure these provisions are followed, the violation of each should be punishable with criminal penalties, the particulars of which are left to Congress' discretion. Therefore, in formulating an ideal kill switch law at the federal level, Congress should include supplemen-

342. *See supra* Part III.A.1.
343. SECURE OUR SMARTPHONES, *supra* note 4.
344. *See* discussion *supra* Part III.A.1.
345. Shaer, *supra* note 19.

tary provisions similar to those in Minnesota's kill switch law, aiming to disrupt the stolen smartphone black market.

b. Takeaways from California's Legislative Approach

California's kill switch law is perhaps a greater indicator of what Congress should avoid than what Congress should incorporate into a federal kill switch law. California's kill switch law, which creates a legal process for the government to access and engage kill switches to disable individuals' smartphones, poses a clear threat to civil liberties constitutionally protected by the First Amendment.[346] The risk of abuse regarding this provision of California's kill switch law is simply too high to justify its existence.[347]

Congress unequivocally should not include such a provision in a federal kill switch law; only an authorized user should be allowed to engage or disengage a kill switch on their device. Instead, Congress should include a provision that overrides California's, embodying a statement similar to the following: no entity, including any entity that is a part of the federal government or any state government, shall be allowed to access, engage, disengage, or otherwise utilize a smartphone kill switch, except for an authorized user; unless permission is granted to such entity by an authorized user. Therefore, California's kill switch grant of privileges to government officials, albeit in limited circumstances, should be both avoided and revoked by Congress when formulating an ideal federal kill switch law.

California's kill switch law is not wholly off base. The specific kill switch provision, calling for an opt-out kill switch, is exactly what should be incorporated into a federal kill switch law, and is indeed what the Smartphone Theft Prevention Act already contains.[348] A federal opt-out kill switch law offers a greater deterrent effect than an opt-in version might, and ensures the maximum number of users have a kill switch equipped on their device.

An opt-out kill switch provision eliminates users who do not have a kill switch equipped on their device due to technical incapability or negligence.[349] As for the small fraction of users who would rather not have a kill switch, for fear of hackers or whatever other reason, they may simply opt-out to attain their preference. Therefore, akin to California's legislative approach, Congress should include an opt-out kill switch provision, making it mandatory for every smartphone sold at retail in the United States to come equipped with a kill switch as a default setting.

346. *See* U.S. CONST., amend. I; *see also* discussion *supra* Part III.A.2.
347. *See* discussion *supra* Part III.A.2.
348. *See* discussion *supra* Part III.C.1.
349. *See* discussion *supra* Part III.A.2.

V. CONCLUSION

Countless devices stolen, billions of dollars wasted,[350] personal information revealed, peace of mind destroyed, fellow citizens lost—all casualties of owning truly life-altering pieces of technology—smartphones.[351] Too long has the smartphone theft epidemic plagued the American people. Yet pioneers among us, Minnesota and California, have forged a way towards a safer future, enacting the first smartphone kill switch laws nationwide.

Though to some degree, Minnesota and California stumbled in their legislative approaches, the track is now set for a passing of the torch. Congress alone has the power to combat the smartphone theft epidemic; Congress alone can shield the nation with a federal kill switch law.

First, like Minnesota, Congress must unleash an arsenal of piecemeal anti-theft legislation, restricting illegitimate transactions and disrupting the smartphone black market economy. Second, Congress must cover the Achilles heel of California's legislative approach, and prevent government entities from disabling individuals' smartphones. Third, with the sword of California's legislative approach, Congress must drive deep into the heart of the smartphone theft epidemic, and enact an opt-out kill switch law to deter thieves and protect consumers. Therefore, by pursuing a "holistic approach [and] embrac[ing] an array of complimentary techniques,"[352] Congress can, with any luck, fix the smartphone glitch, achieving consumer protection, by way of legislative kill switch.

350. *See* DUCKWORTH, *supra* note 12, at 2–3.
351. *See* discussion *supra* Part II., III.
352. Shaer, *supra* note 19.