LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 4 FALL 2016 ISSUE 1

COULD KILL SWITCHES KILL PHONE THEFT?

SURVEYING POTENTIAL SOLUTIONS FOR SMARTPHONE THEFT

Matt Rietfors & Vikram Iyengar[1]
Stanford Law School

INTRODUCTION

In 2013, 3.1 million Americans were victimized by smartphone theft, nearly double the total of a year before.[2] The problem is particularly acute in major cities, where smartphone theft is now involved in 30 to 40 percent of all robberies.[3] In San Francisco, smartphones were stolen in more than half of total robberies in 2012.[4] These thefts cost

[1] The authors thank Phil Malone, Professor of Law and Director of the Juelsgaard Intellectual Property and Innovation Clinic at Stanford Law School, and Jef Pearlman, Clinical Supervising Attorney and Lecturer in Law at Stanford Law School, for their guidance and helpful comments on this Note.

[2] *3.1 Million Smart Phones Were Stolen in 2013, Nearly Double the Year Before*, CONSUMER REPORTS (April 17, 2014), http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html.

[3] H.R. 962 § 1(a), 2014 Leg. Counsel, Reg. Sess. (Cal. 2014).

[4] *Id.* § 1(d).

consumers approximately $30 billion a year according to the FCC,[5] and law enforcement officials worry that they pose significant public safety costs as well. This is not hard to believe, given that 68% of theft victims would put themselves in some degree of danger to recover their phone.[6] With 1 in 10 device owners now victims,[7] the shocking growth of smartphone theft and its attendant financial and safety costs has created an apparent epidemic.

But, is this theft problem really unique to smartphones? The increase in stolen smartphones may simply reflect the increase in smartphone ownership. In other words, thieves may not specifically plan ahead and single out phones to steal. Other electronic devices such as laptops and tablets are also stolen regularly, but smartphone theft may occur at a greater rate for a variety of reasons: they are smaller, easier to mine data from, easier to repurpose post-theft, and people carry them around more routinely with less precaution.

Whether the theft problem is unique to smartphones or not, a solution that reduces theft of smartphones in particular and electronic devices in general is desirable if it is possible. Perhaps the most obvious response is to make stolen phones less valuable. If thieves cannot access owner data or connect phones to cellular or Wi-Fi networks, they may be less inclined to risk stealing a smartphone. This is the crux of the leading anti-theft proposal. By mandating implementation of a "kill switch" that can remotely disable a phone's essential features, legislatures and public officials hope to disincentivize stealing and reverse the theft trend.

This paper analyzes the potential efficacy of current proposals to deter smartphone theft and the broader implications they may have. It surveys arguments of

---

[5] Smartphone Theft Prevention Act, H.R. 4065, 113th Cong. § 2(1) (2014).

[6] *Phone Theft in America*, LOOKOUT MOBILE SECURITY (May 7, 2014), https://www.lookout.com/resources/reports/phone-theft-in-america.

[7] *Id.*

leading stakeholders, examines the relevant literature on technological feasibility and consumer behavior, and assesses the potential pitfalls and shortcomings in implementing a cohesive, effective policy. Developing a sound theft-deterrence policy requires clarity on and a better understanding of kill switch technology, other potential approaches such as carrier registries, smartphone theft psychology, and the mechanics of the smartphone black market. This paper represents the first attempt at studying and answering these questions.

I. HISTORY OF THE KILL SWITCH DEBATE

A. A CALL TO MANDATE KILL SWITCHES AND SAMSUNG'S RESPONSE

The movement to mandate the deployment of a kill switch, a technological method to render a stolen smartphone and its data unusable, first gained prominence in 2012 when smartphone theft began increasing rapidly. The Secure Our Smartphones (SOS) campaign, led by New York Attorney General Eric Schneiderman and San Francisco District Attorney George Gascon, gathered supporters around the country as it pressured phone carriers and manufacturers to introduce a default kill switch in new phones.[8]

Following this pressure, on July 18, 2013, Samsung proposed adding the LoJack security system, including a kill switch designed by Absolute Software, to its smartphones at an additional cost to consumers.[9] The LoJack system would work through a desktop app and code buried with the phone's firmware. However, because most smartphones in the U.S. are sold by carriers,

---

[8] Office of the N.Y. Attorney General Eric T. Schneiderman, *Secure Our Smartphones (S.O.S.)*, http://www.ag.ny.gov/feature/secure-our-smartphones-sos.

[9] Martyn Williams, *U.S. Carriers Rejected 'Kill Switch' Technology Last Year*, COMPUTERWORLD (Feb. 24, 2014 08:42 AM), http://www.computerworld.com/s/article/9246557/U.S._carriers_rejected_39_kill_switch_39_technology_last_year.

Samsung needed the carriers' approval to pre-install LoJack on phones. None of the five major carriers agreed.[10]

B. CTIA'S PROPOSED ALTERNATIVES AND RESPONSES THERETO

Carriers and manufacturers, through their representative CTIA—The Wireless Association, initially denounced the SOS kill switch initiative and instead created a collaborative registry aimed at eliminating the stolen phones resale market. Eventually, however, intensifying scrutiny prompted the CTIA to modify its position. It recently created the Smartphone Anti-Theft Voluntary Commitment, in which signatories declare their intent to make kill switch functionality available on all of their new phones by July 2015.[11]

But many kill switch advocates argue that this voluntary commitment falls short. Citing the need for ubiquity to ward off thieves, consumer rights advocates and a handful of state legislatures have pushed for mandatory, rather than voluntary, adoption of kill switches. One such bill, California's S.B. 962, finally passed the state senate in May 2014 (and was signed into law on August 25, 2014)[12] after Apple, Samsung, Microsoft, and Google withdrew opposition on the conditions that the implementation deadline be pushed back to July 2015 and tablets be dropped from the bill. These companies already include software on their phones that allows owners to lock or erase devices from afar, but they generally accord with the CTIA's position of keeping anti-

---

[10] Press Release, Eric T. Schneiderman, Attorney General of New York, (Dec. 11, 2013), http://www.ag.ny.gov/press-release/ag-schneiderman-requests-information-leading-wireless-carriers-decision-reject-anti.

[11] Smartphone Anti-Theft Voluntary Commitment, CTIA—THE WIRELESS ASSOCIATION, (accessed February 3, 2015), http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

[12] H.R. 962, 2014 Leg. Counsel, Reg. Sess. (Cal. 2014).

theft measures voluntary and up to the discretion of consumers.

C. FINDING A WAY FORWARD

While most interested parties in the debate thus appear to endorse a kill switch option, kill switch implementation is not failsafe. The question remains whether current statutory kill switch mandate proposals "will effectively deter theft without jeopardizing public safety, personal privacy, and civil liberties, or causing other undesirable consequences."[13] It is entirely possible that a kill switch solution could create as many problems as it solves.

II. OPINIONS OF STAKEHOLDERS ON KILL SWITCHES

The debate over curbing smartphone theft has engendered a good deal of controversy. Some legislators have unabashedly attacked carriers and manufacturers for opposing a public safety law in order to retain profits arising from replacement of stolen phones. The carriers and manufacturers respond by arguing that they present consumers with a variety of security options, to which a mandatory kill switch would only be a costly and burdensome addition. On the sidelines of the debate are a number of privacy activists and technologists who worry that mandating kill switches may enable the possibility of widespread hacking or discourage innovation. Finally, smartphone owners provide insights about feasibility of security options with their relative apathy towards anti-theft measures.

---

[13] California Senate, Energy, Utilities and Communications Committee, March 24, 2014, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB962&search_keywords (click Bill Analysis tab, then click the link titled "03/28/14 – Senate, Utilities And Communications").

A. LEGISLATORS AND PUBLIC SAFETY OFFICIALS SUPPORT STRONG KILL SWITCHES

Following the beginning of the Secure Our Smartphones campaign, New York Comptroller Thomas DiNapoli publicly pressured Google, Microsoft, Apple, and Samsung to declare what they were doing to "assure public officials that [they are] acting responsibly" in response to the rise in smartphone theft or else face divestment of nearly $3 billion from the state of New York.[14] The comments confronted the companies with acting "disinterested when it comes to collaborating with law enforcement agencies in the effort to develop a meaningful technological solution that would effectively eliminate the secondary market in which criminal elements realize their profits."[15]

Following a decision by the major carriers to reject Samsung's kill switch in late 2013, supporters of a mandatory kill switch became even less diplomatic in their allegations. San Francisco District Attorney George Gascón accused the carriers of rejecting the Samsung solution "so they could continue to make money hand over fist on insurance premiums."[16] Insurance and phone replacement costs are major components of carrier profits, comprising $7.8 billion and $30 billion in revenue, respectively, of the $69 billion the industry nets every year.[17] Captain Jason Cherniss of the San Francisco Police

---

[14] Letters from Thomas P. DiNapoli, Comptroller of the State of New York, to Google, Microsoft, Apple, and Samsung (June 11, 2013), http://www.ag.ny.gov/sites/default/files/pdfs/features/sos/SOS-Letters.pdf.

[15] *Id.*

[16] Paul Wagenseil, *Smartphone Kill Switch: What It Is, How it Might Work*, TOM'S GUIDE (May 14, 2014 9:40AM), http://www.tomsguide.com/us/ smartphone-kill-switch-faq,news-18772.html (internal quotations omitted, quoting Gascón).

[17] Rachel Swan, *The Life of a Stolen Phone: For the Smartphone Industry, Theft is Part of the Business Model*, S.F. WEEKLY (April 23,

Department says the police have "tried to blow the whistle on this for years . . . [while] companies have had the ability to prevent for years . . . [and] people have been violently robbed - even killed - and millions of dollars have changed hands on the black market."[18] Secure Our Smartphones leader Eric Schneiderman blasted the carriers for "knowingly dismiss[ing] technology that could save lives."[19]

B. OBJECTIONS TO MANDATORY IMPLEMENTATION

But the carriers (and manufacturers) see kill switches as not only technologically uncertain, but also as potentially becoming conduits of new problems. The CTIA has expressed concern that ubiquitous kill switches would give hackers or other undesired parties the ability to disable entire groups of phones, with particular susceptibility for "random customers as retaliation by a variety of persons or entities."[20] Manufacturers claim that they have already made commercially available and promoted affordable anti-theft solutions, including Apple's Find My iPhone and Activation Lock and Samsung's Reactivation Lock. The major carriers of the CTIA, though initially rejecting wholesale Samsung's kill switch proposal in 2013, recently agreed to make available kill-switch solutions on a consumer-voluntary basis.[21]

This voluntary-as-opposed-to-mandatory proposal accords with the position of many technologists and privacy rights activists who worry that consumers may be

---

2014), http://www.sfweekly.com/2014-04-23/news/smartphone-theft-apple-at-t-iphone/full/.

[18] *Id.*

[19] Schneiderman, *supra* note 10.

[20] CTIA--The Wireless Association, *Why a "Kill Switch" Isn't the Answer* (accessed February 3, 2015), http://files.ctia.org/pdf/Why_a_Kill_Switch_Isn_t_the_Answer.pdf.

[21] CTIA--The Wireless Association, *Smartphone Anti-Theft Voluntary Commitment* (accessed February 3, 2015), http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

coerced into increased susceptibility to hackers. Further, consumers already have a variety of security tools available to them, and legally sanctioning more pathways for Big Brother (or Anonymous) to intrude on consumers' ability to communicate is concerning, particularly in light of recent crackdowns in Egypt, BART protests, and Occupy Wall Street. In this regard, consumer safety may be diminished by an inability to reach emergency services or dependent contacts.

Some technologists also fear that mandatory technology may create a barrier to entry for smaller innovators in the smartphone industry or even more simply create more costs than benefits. In comments filed with the California Senate, the San Jose Silicon Valley Chamber of Commerce reminded legislators "to be sensitive to the regulatory environment necessary for innovation" and asserted that different technology mandates in states across the country "could create considerable market barriers for innovative manufacturers and the consumers they serve, and mandating technology is usually a recipe for the creation of an anticompetitive and anti-consumer choice environment."[22]

C. CONSUMER BEHAVIOR PROVIDES LITTLE CLARITY ON THE POTENTIAL EFFECTIVENESS OF A MANDATORY KILL SWITCH

In the midst of this debate, smartphone owners--perhaps the stakeholders with the most at stake--seem to collectively demonstrate the least bit of interest. Less than half of smartphone users secure their phones with a homescreen passcode, and among those that do, the most popular passcodes are among the simplest: 1111, 0000, and

---

[22] Comments of San Jose Silicon Valley Chamber of Commerce in Senate Floor Analysis, May 7, 2014, California State Senate, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB962&search_keywords (click Bill Analysis Tab, then click the link titled "05/07/14 – Senate Floor Analysis).

1234.[23] Aggregating the passcode with other phone security measures such as antivirus software and data backup, 34% of smartphone owners take no measures at all.[24] This seeming indifference may support the notion that a mandatory anti-theft solution could produce radical effects, but it may also reveal that smartphone users simply prefer more straightforward usage with fewer security barriers. Regardless of what it means, interested parties on both sides of the table have mobilized consumer behavior data to support their positions. Currently proposed kill switch bills in state and federal legislatures, for instance, base their rationales in consumer protection.

III. HOW THE LEGISLATION CONCEIVES OF KILL SWITCHES

While the various bills[25] active in state legislatures and Congress differ in how they describe the ideal features of kill switches, they all allude to kill switches vaguely as a sort of "technological solution." The pending federal bill goes even further, exempting from the mandate any smartphone provider that incorporates technology that "accomplishes the functional equivalent of the [defined technological] function."[26] By keeping the definition broad, the bills enable companies to use technology compatible with their business and design strategies, hence making it more palatable to comply with the mandate. However, the broad definitional scope also reflects a degree of legislative uncertainty on what constitutes the most effective functionality. Reflecting this point, the five pending and passed bills--California,

---

[23] Corinne Iozzio, *Kill Switches Will Save Your Smartphone*, POPULAR SCIENCE (May 5, 2014), http://www.popsci.com/article/technology/kill-switches-will-save-your-smartphone.

[24] Stephen Schenck, *US Smartphone Thefts Explode, Nearly Doubling Since 2012*, POCKETNOW (April 18, 2014, 5:18 PM), http://pocketnow.com/2014/04/18/smartphone-theft.

[25] *See* Appendix for excerpts of selected bill text.

[26] Smartphone Theft Prevention Act, H.R. 4065, 113th Cong. (2014).

Minnesota, New York, Illinois, and the federal bill--all have important differences.

While all of the bills agree that a kill switch must involve software or hardware (or a combination of both) that can render inoperable the essential features of the device to an unauthorized user, they vary in their interpretation of "inoperability" and "essential features." The bills generally accord that the kill switch should disable voice communications, Internet accessibility, and application functionality, but the proposed Illinois and federal bills go further to clarify that this must be achieved "even if the device is turned off or has the data storage medium removed."[27] In this regard, the Illinois and federal bills would require a permanent solution that prevents re-programmability after the phone is rendered inoperable.

The treatment of data also reveals the bills' different conceptions of kill switch functionality. The California bill, for instance, is silent on the technology's effect on user data, whereas the other bills require the kill switch to either lock or disable the stored data. The Minnesota bill requires the kill switch to lock all data, but retain future accessibility, while the Illinois bill would require permanent removal. The federal bill splits the difference between the two and leaves the option open to manufacturers and providers.

Compliance enforcement also varies from bill to bill. Each bill, aside from Illinois's, supports a per-phone monetary penalty levelled against those who manufacture and sell non-conforming phones, while Illinois would require violating providers to insure the phones for theft at no cost to the customer. Minnesota's bill contains additional provisions that prevent purchasers of used or secondhand phones from buying in cash and requires these buyers to keep records of their purchases.

In total, the current legislative proposals are united in calling for a mandate on some sort of technological solution that would help consumers render some subset of

---

[27] *Id*. *See also* IL S.B. 3539 ("SIM card or data storage medium removed").

key features inoperable on a stolen phone. The various approaches on specifics, from definitional differences to dealing with data on a permanent or reversible basis, underscores some of the uncertainty on how a kill switch could work most effectively.

IV. TECHNICAL ISSUES INVOLVED WITH IMPLEMENTING KILL SWITCHES

The state and federal kill switch legislation as well as the Voluntary Commitment from the CTIA both suffer from a dearth of detail about technical specifications and how a kill switch would be implemented. The bills simply call for any hardware or software "technological solution" that is mandatory and can survive a factory reset.[28] However, a kill switch solution implemented entirely in software will likely not work flawlessly, especially if the software is implemented at a high level of abstraction—in the operating system (OS) or as an app.

A. KILL SWITCHES IMPLEMENTED IN SOFTWARE

Software kill switches depend on users running the latest OS and software patches necessary to enable the kill switch feature to work. For example, Apple's Find My iPhone[29] app and Activation Lock[30] feature in iOS 7 were designed to function as a kill switch. Once enabled, Activation Lock is designed to make a stolen iPhone unusable even if the phone is reset. However, only 85% of iPhones ran iOS 7 at the time the first smartphone bills got introduced.[31] Therefore, there was still a large chance that

---

[28] *See, e.g.*, H.R. 962, 2013 Leg. Counsel, Reg. Sess. § 2(b)(1) (Cal. 2013).

[29] Apple Computer Inc., *Find My iPhone*, http://www.apple.com/icloud/find-my-iphone.html.

[30] Apple Computer Inc., *iCloud: Activation Lock*, http://support.apple.com/kb/PH13695.

[31] Christian Zibreg, *According to Apple, 85 percent of iPhone, iPod touch and iPad devices run iOS 7*, IDOWNLOADBLOG (Mar. 24, 2014), http://www.idownloadblog.com/2014/03/24/apple-85-percent-devices-ios-7.

a stolen iPhone either did not run iOS 7 or have the Find My iPhone app enabled. For example, a recent theft victim had shut off the Find My iPhone app after reading about how it had been abused by a hacker to remote-wipe tech writer Mat Honan's iPhone, iPad, and laptop.[32] With the large number of smartphone offerings, OSs, and app versions on the market today, designing a set of reasonably foolproof kill switch apps that have similar levels of protection for users across industry platforms will require a significant standards-setting initiative and frequent communication between smartphone manufacturers and carriers on bug fixes, technology updates, and software patches.

California's kill switch bill and the CTIA's Voluntary Commitment would require any smartphone manufactured in the United States for retail sale after July 1, 2015 to have a kill switch (the latter on a voluntary commitment). However, most users keep their smartphone models for two to three years. Hence, even after July 1, 2015, there will be millions of smartphones that were purchased previously running older OS versions that do not support the kill switch. Moreover, iPhones running iOS 7 (with the kill switch) look almost identical to models without it. Therefore, smartphone thieves will likely not be deterred by kill switches for a few years after July 1, 2015, and will take the chance that a given smartphone does not have a properly functioning kill switch. Even if a stolen iPhone has the kill switch app installed and functional, if a user waits too long to run Find My iPhone, that can give the thief time to unload the device. (The average duration of time from theft to recognition of theft is one hour.)[33]

---

[32] Rob Pegoraro, *Will Apple's 'kill switch' tamp down iPhone thefts?*, USA TODAY (May 4, 2014, 7:00 AM), http://www.usatoday.com/story/tech/columnist/2014/05/04/will-apples-kill-switch-tamp-down-iphone-thefts/8577215.

[33] *Phone Theft in America*, LOOKOUT MOBILE SECURITY (May 7, 2014), https://www.lookout.com/resources/reports/phone-theft-in-america.

B. SOFTWARE KILL SWITCHES CAN BE BROKEN INTO

Thieves may also be able to defeat kill switches if the user has not installed the latest software security patch. For example, Apple recently put out a security fix for a vulnerability that allowed a thief to disable Find My iPhone on iOS 7 without a password.[34] That defense was also circumvented in cases where a user did not set a screen-unlock passcode.[35]

Most recently, hackers have even broken into Apple's Activation Lock installed on the latest iOS 7 with all the latest software patches. The two hackers who call themselves doulCi (iCloud, fashioned roughly backwards), claimed to have made the workaround "for people who have retrieved their lost or stolen iDevice, in an effort to recover access to contacts, email, notes, and more."[36] The system works by "plugging [an] iPhone or iPad into a computer and altering a file inside . . . trick[ing] the device into connecting to the hackers' server instead" and causing the phone to unlock.[37] Shortly following the release of the doulCi hack, pictures on social media appeared "show[ing] that thousands of locked iPhones around the world [were] bypassed using the tool just [in the first day]."[38] Most of the tweets thanking the two hackers come from outside of the U.S, where stolen smartphones are shipped and sold at a premium on the black market.[39] For

---

[34] Carly Page, *iOS 7 Exploit Disables Find My Iphone Without a Password*, THE INQUIRER (Feb. 7, 2014, 1:10 PM), http://www.theinquirer.net/inquirer/news/2327573/ios-7-exploit-disables-find-my-iphone-without-a-password.
[35] Pegoraro, *supra* note 32.
[36] Stephanie Mlot, *Hackers Breach Apple's Activation Lock*, PC MAGAZINE (May 22, 2014, 9:50 AM), http://www.pcmag.com/article2/0,2817,2458399,00.asp.
[37] Jose Pagliery, *Hackers Can 'Un-Brick' Stolen iPhones*, CNNMONEY TECH 30 (May 21, 2014, 1:37 PM), http://money.cnn.com/2014/05/21/technology/security/icloud-hack/index.html.
[38] *Id.*
[39] Alex Heath, *Apple Too Late to Stop Massive iCloud Breach, Hackers Claim*, CULT OF MAC (May 21, 2014, 4:46 PM),

example, an iPhone 5S that costs $707 in the US costs $1,090 in Jordan and $1,196 in Brazil.[40] The doulCi hack suggests that software kill switches on phones are certainly not immune, even from the work of a couple of rogue hackers.

C. REMOTE ACTIVATION OF KILL SWITCHES

A true software kill switch, as opposed to a simple lock-and-wipe app, would require sending a signal to the phone over the cellular network or the Internet to "brick" the phone by deleting the OS or by sending out a poisoned firmware update. Absent of physical damage to the hardware, the phone could still be made functional by installing a new OS or by using special tools to fix the firmware.[41] iPhones, in particular, are "jailbroken" routinely, with the smartphone running a knock-off OS. Therefore, a purely software-based approach to render a smartphone forever nonfunctional is unlikely to work.

A kill switch implemented in software can also be avoided. A thief would have to shut the smartphone off immediately after he steals it, which most experienced thieves already do to avoid tracking software. The thief could alternatively place the stolen smartphone into a Faraday Bag[42] that blocks Wi-Fi, cellular, and GPS signals and wait until he reached a location without a cellular signal, e.g., a metal shed or basement. At that point, the SIM card can be removed and discarded, the phone can be turned on, the data wiped, and the 15-digit International

---

http://www.cultofmac.com/280189/icloud-hacker-calls-apples-response-little-late.

[40] Swan, *supra* note 17.

[41] Jesse Emspak, *Why a smartphone 'kill switch' won't deter theft*, MOTHER NATURE NETWORK (Aug 27, 2013, 02:19 AM), http://www.mnn.com/green-tech/gadgets-electronics/stories/why-a-smartphone-kill-switch-wont-deter-theft.

[42] Kelsey D. Atherton, *Hide From GPS With This Signal-Blocking Phone Case*, POPULAR SCIENCE (Aug. 6, 2013, 1:15 PM), http://www.popsci.com/gadgets/article/2013-08/how-protect-yourself-your-phone.

Mobile Equipment Identity (IMEI) number changed.[43] The carrier network, and kill switch that depends on it, would be totally ineffective.

D. KILL SWITCHES EMBEDDED IN HARDWARE

Samsung proposed a more permanent solution, the Absolute LoJack kill switch,[44] to carriers in 2013, but the carriers rejected the proposal. The Absolute LoJack method embeds the kill switch in the smartphone's BIOS (firmware) that can withstand a factory reset and wiping or replacing the hard drive. However, hacker websites[45] offer instructions for computer-savvy hackers on how to edit a smartphone's BIOS to disable LoJack. Hence, a truly tamper-proof kill switch would have to be either embedded in read-only memory (ROM) or built into the integrated circuits (ICs) on the motherboard itself. The logic on an IC could be programmed to (1) cause the IC to malfunction; (2) reset the memories; or (3) destroy the IC by creating a short in the circuit. Because the kill switch would be within the IC, detecting it and disabling it would be near impossible.[46] In addition, the kill switch would have to be embedded on *every* motherboard manufactured so that if a thief tried to replace the motherboard on a smartphone, the new replacement motherboard would also have the kill switch. At this point, working around the kill switch would still be possible for the thief.

---

[43] Emspak, *supra* note 41.

[44] *Absolute Persistent Security Software. The Only Solution That Can Survive a Factory Reset*, ABSOLUTE SOFTWARE, http://lojack.absolute.com/en/persistent (last visited May 30, 2014).

[45] *See, e.g.*, *How to Remove Computrace LoJack*, FREAKY ACRES, http://www.freakyacres.com/remove_computrace_lojack (last visited May 30, 2014).

[46] Email from Mark Tehranipoor, Charles H. Knapp Associate Professor of Electrical & Computer Engineering, University of Connecticut, to authors (May 30, 2014, 11:06 AM) (on file with authors).

However, because a new motherboard costs upwards of $100,[47] it might serve as a sufficient deterrence to theft.

E. HARDWARE REDESIGNS THAT COULD WORK

Modern electronic devices, such as smartphones, have sleep states that are in between fully on and fully off. In sleep mode, some circuits on the smartphone are powered up and others are powered down.[48] "These modes often allow the device to wake up autonomously if certain conditions are met, such as pressing a certain key or even receiving certain data over the Internet. . . ."[49] Therefore, a kill switch that could be activated to wake up and "brick" the smartphone even when the smartphone were switched off by a thief would be useful. In addition, a hardware redesign to thwart thieves that remove the smartphone battery to evade tracking could be to insert secondary power sources within the apparatus. "Some phones [already] use an additional battery for memory management; it's unclear whether this battery could be used by logging and/or tracking systems. . . ."[50] Such a secret secondary power source could be used to power tracking apps and the kill switch.

F. FOOLPROOF BUT EXPENSIVE SOLUTIONS

Militaries around the world have designed "remote shut-down" solutions on defense systems since at least 2008 to disable ICs on equipment that might fall into hostile hands. These generally consist of kill switches or

---

[47] iPhone 5 Replacement Motherboards, EBAY, http://www.ebay.com (search "iphone 5 replacement motherboard") (last visited May 30, 2014).

[48] Heather Murphy, *Why Snowden Asked Visitors in Hong Kong to Refrigerate Their Phones*, N.Y. TIMES (Jun. 25, 2013, 9:41 AM), http://thelede.blogs.nytimes.com/2013/06/25/why-snowdens-visitors-put-their-phones-in-the-fridge/?_r=0&pagewanted=all (quoting Seth Schoen, Senior Staff Technologist, Electronic Frontier Foundation).

[49] *Id.*

[50] *Id.*

backdoors. A military-style kill switch manipulates the system's software or hardware to cause the system to die outright, for example, to shut off an F-35's missile-launching electronics.[51] A backdoor, on the other hand, lets the designer gain access to the system to disable or enable a specific function. Because a backdoor does not shut down the entire system, hostile users remain unaware of the intrusion. For example, a designer could use it to bypass battlefield radio encryption. Similarly, smartphone manufacturers or carriers could use a backdoor to continue tracking a thief while blocking access to the owner's sensitive data. However, military-style designs, while foolproof, would likely prove too expensive for commercial smartphones unless breakthroughs in technology and design occur.

Boeing recently filed documents with the FCC to build a tamper-proof android smartphone it calls the "Black" phone. The "Black phone will be sold primarily to government agencies and companies . . . related to defense and homeland security," says a letter accompanying the filing.[52] There are no serviceable parts on Boeing's Black phone and any attempted servicing or replacing of parts would destroy the product. The phone is sealed with epoxy around the casing and with screws, the heads of which are covered with tamper proof covering to identify attempted disassembly. While such a device would provide high security indeed, the need for commercial devices to be serviced or repaired likely precludes a specialized solution like Boeing's for commercial

---

[51] Sally Adee, *The Hunt for the Kill Switch*, IEEE SPECTRUM (May 1, 2008, 7:57 PM), http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

[52] Letter from Bruce A. Olcott, *The Boeing Company, Supplemented Request for Confidential Treatment FCC Identification Number H8V-BLK1 (Model: BLACK)*, to Joe Dichoso, Chief Equipment Authorization Branch, Office of Engineering and Technology, Federal Communications Commission, https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=2202965.

smartphones. In addition, Boeing will not provide technical and operational information about the product to the general public for security purposes.[53] Technical information distributed at trade shows will be protected by non-disclosure agreements. With the proliferation of hacker sites instructing the public on jailbreaking smartphones and evading kill switches, commercial smartphone companies might soon decide to follow this route in the future.

Finally, researchers at Rice University and the University of California, Los Angeles recently invented a new method to protect integrated circuits (IC) against piracy. The new method exploits the inherent variability in modern IC manufacturing to create a unique identifier for each IC and integrate the identifier into the IC's functionality.[54] However, while this novel method solves the IMEI erasing problem and is attack-resilient, it would likely lead to a large overhead cost for smartphone manufacturers and would be difficult to standardize across smartphone platforms.

V. NON-KILL-SWITCH SOLUTION: CARRIER REGISTRIES AND MOBILE DATA MANAGEMENT

A. CARRIER REGISTRY OPERATION

Seeking to deflect legislation that would mandate kill switches for all smartphones, and seeking to avoid dealing with the technical challenges enumerated above, U.S. carriers implemented databases in November 2013 that use unique GSM and LTE (advanced GSM) smartphone ID numbers to prevent stolen smartphones from being re-activated on GSM or LTE networks in the

---

[53] *Id.*

[54] Yousra Alkabani, et al., *Remote Activation of ICs for Piracy Prevention and Digital Rights Management*, Proceedings of the Int'l Conference on Computer-Aided Design of Integrated Circuits and Systems 674-77 (2007), http://www.cs.ucla.edu/~miodrag/papers/Alkabani_ICCAD_2007.pdf.

U.S. and on appropriate international LTE networks.[55] At present in the U.S., consumers that lose their smartphones may call their service provider and have service suspended to the smartphone.[56] However, it is the consumer's responsibility to know the device's make, model number, serial number, and unique device identification number (either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number).[57] Different smartphone models and carriers may use GSM networks, CDMA networks, LTE networks, or a mix of the three.[58] Therefore, a stolen smartphone that is blocked on one registry could be activated on a registry using a different network standard.

Additionally, consulting the registries and blocking activation of phones reported as stolen is a *voluntary* action of carriers.[59] Remote phone location, locking, and data-wiping services depend entirely on whether the manufacturer and carrier provides them on the particular smartphone model; the features are not uniformly offered on all models or by all carriers.[60] Manufacturer or third-

---

[55] Letter from Brian M. Josef, *CTIA Stolen Smartphones Status Update*, to Kris Monteith, Acting Bureau Chief, Consumer and Governmental Affairs Bureau, Federal Communications Commission, http://www.ctia.org/docs/default-source/default-document-library/july-2013.pdf?sfvrsn=0.

[56] FCC, *How to Report a Lost or Stolen Smart Device*, http://www.fcc.gov/stolen-phones-contact-numbers.

[57] FCC, *Protect Your Mobile Device*, http://www.fcc.gov/guides/stolen-and-lost-wireless-devices.

[58] European Telecommunications Standards Institute (ETSI), *Mobile Communications*, http://www.etsi.org/technologies-clusters/technologies/mobile.

[59] Daniel E. Dilger, *Apple Gov't rep says next two iPhones were designed under Steve Jobs*, APPLEINSIDER (April 01, 2013, 12:03 PM), http://appleinsider.com/articles/13/04/01/apple-govt-rep-says-next-two-iphones-were-designed-under-steve-jobs.

[60] *See e.g.*, AT&T, *Replace your lost or stolen device and suspend service*, http://www.att.com/esupport/article.jsp?sid=52993&cv=820&_requestid=1370759#fbid=COrGqYlcbAL.

party apps available for some models today can locate a stolen device from a computer, lock the device to restrict access, wipe sensitive data from the device, and make the device emit a loud sound ("scream") to help the police locate it. However, carriers and manufacturers are not required to make such apps available on all phones or on all networks.[61]

Once service is suspended on the smartphone, the consumer cannot wipe or lock it. Monthly plan charges continue while service is suspended, and the consumer must have bought insurance ahead of time to get the smartphone replaced.[62]

B. AUSTRALIA'S REGISTRY PROGRAM HAS PRODUCED RELATIVE SUCCESS

Australia implemented an IMEI blocking program a decade ago and has deemed it successful at deterring theft with "net blocking activity [falling] by nearly 25% from 169,000 mobile handsets blocked to 127,750 [from 2004-2011] . . . against the background of an 80% increase in the number of mobile services in operation over this period."[63] The IMEI is an integral phone "fingerprint" that is transmitted whenever the phone is used. Supporters of an IMEI system claim that it may prove more failsafe than mandatory kill switches. Speaking with American media, Randal Markey of the Australian Mobile Telecommunications Association highlighted the ease of implementing and operating a shared database, which just requires collaboration amongst carriers, and the relative

---

[61] *Supra* note 57.

[62] *Id.*

[63] Australian Mobile Telecommunications Association, *Australian Anti-Theft Mobile Phone Technology Highlighted on U.S. Television* (accessed May 21, 2014), http://www.amta.org.au/articles/Australian.anti-theft.mobile.phone.technology.highlighted.on.US.television (additionally noting that "[t]he net blocking figures are derived from subtracting unblocking requests (if the handset is subsequently found and returned to its legal owner) from blocking requests").

difficulty for unsophisticated thieves to wipe the IMEI number.[64]

C. PROBLEMS WITH A REGISTRY SOLUTION

However, there are a number of problems plaguing voluntary carrier registries. Many consumers do not know about them and do not report stolen phones. Many stores or fly-by-night operations "will jailbreak a stolen phone 'no questions asked,' and thieves can then re-activate the smartphone with a smaller carrier that is not participating in the registry."[65] Carrier registries may thus simply encourage more black market workarounds. Moreover, the registries mainly apply in the U.S. and Europe and could encourage thieves to ship stolen phones to other areas, where they are more valuable because of export restrictions and tariffs. Additionally, any projected effect of IMEI blocking on theft depends on the assumption that thieves require cell service at all, not just in the registry-covered areas like the U.S. and Europe. Deterrence of an IMEI system may fail to prevent thieves who simply wish to profit off of hardware resales, user data mining, or use of other smartphone functions (digital music, camera, etc.). A hack-proof mechanism to track and shut down stolen devices anywhere in the world, regardless of which carrier is used and without burdening the consumer with the responsibility of purchasing and downloading apps (or

---

[64] C.W. Nevius, *An Easy Way to Curb Smart Phone Thieves*, S.F. GATE (Dec. 3, 2011), http://www.sfgate.com/bayarea/nevius/article/An-easy-way-to-curb-smart-phone-thieves-2344797.php.

[65] Josh Harkinson, *For Apple and the Phone Companies, "All a Theft Means Is Another Sale,"* MOTHER JONES (Mar. 18, 2013 8:58 AM), http://www.motherjones.com/mojo/2013/03/stolen-iphone-theft-imsi (describing San Francisco District Attorney George Gascón's views on mobile device makers and carriers doing little to fix the problem).

remembering the smartphone's 15-digit IMEI number), would likely be a stronger deterrent to smartphone theft.[66]

D. MOBILE DATA MANAGEMENT

Growing employee demand for bringing their personal smartphones to work has driven security-minded employers to use Mobile Data Management (MDM) services provided by third-party vendors. MDM provides increased security for both the devices and the enterprise they connect to by controlling and protecting the data and configuration settings for all mobile devices in the network.[67] MDM solutions can control the apps installed or available on an employee's personal smartphone and disable the camera when on company premises. In addition, MDM software can lock and wipe a lost or stolen smartphone, display a message on its screen, and cause it to emit a high-volume sound. Other options include a wireless or Bluetooth tether that ties a smartphone to a key fob and locks or wipes the smartphone if it is separated from the key fob by a maximum specified distance.[68] However, MDM solutions do not prevent theft; they merely secure data in the event of theft.

VI. THE MANDATORY KILL SWITCH SOLUTION'S RELATIVE EFFECTIVENESS AT DETERRING THEFT

In theory, implementing a default kill switch in every smartphone is seen as the ideal deterrent to theft because it would decrease the expected value a thief gets from stealing while presenting fewer points of confusion

---

[66] *Id.* (quoting Kevin Mahaffey, Chief Technology Officer, Lookout (a maker of anti-theft smartphone apps,) "That seems like something that is reachable[]").

[67] *BYOD Requires Mobile Device Management*, INFORMATIONWEEK (May 5, 2011, 4:25 PM), http://www.informationweek.com/mobile/byod-requires-mobile-device-management/d/d-id/1097576?.

[68] DEBORAH MORLEY, CHARLES PARKER & JANET LAVINE, UNDERSTANDING COMPUTERS : TODAY AND TOMORROW 597 (2004).

to consumers and fewer available black market workarounds to thieves, fly-by-night operations, or crime syndicates. However, even assuming that a mandatory switch could be implemented without technical difficulties or hacking susceptibility, it may fail to deter thieves for a number of reasons. At the same time, mandating kill switches may help correct, for consumer security, apathy that indirectly encourages theft. Without more information about theft incentives and characteristics, the effects of a kill switch cannot be predicted for certain.

A. THE MANDATORY KILL SWITCH SOLUTION REQUIRES MANY ASSUMPTIONS AND MAY MISINTERPRET THIEVING BEHAVIOR

The premise that putting kill switches in every phone will stop thieves from stealing phones relies upon a number of assumptions, including that: (1) thieves specifically target phones; (2) thieves target phones for their operability and will actually learn of kill switches; and (3) thieves cannot benefit from workarounds, such as hacks, which may pop up from time to time. Because of legislative requirements, any kill switch underpinning these assumptions must also be costless to consumers, leading to another constraint on likely effectiveness since more expensive and potentially more effective solutions are foreclosed.

1. THIEVES MAY NOT SPECIFICALLY TARGET PHONES TO STEAL

First, the increasing incidence of smartphone theft may belie the conclusion that thieves are specifically seeking to steal smartphones. While smartphone theft nearly doubled last year, most of the growth came from large urban areas.[69] It is entirely possible that spikes in

---

[69] Samantha Murphy Kelly, *What's the Worst U.S. City for Smartphone Theft?*, Mashable (Nov. 8, 2012), http://mashable.com/2012/11/08/smartphone-theft-city/ (noting that the top ten locations for smartphone theft are

smartphone theft simply reflects the fact that more theft victims carry visible smartphones in their bags or on their person, or that smartphone owners have become less protective of their phones as they take them all over town.

The former point may have some statistically significant effect, as smartphone ownership has increased from 45% of Americans in 2012 to 58% by the end of 2013.[70] Part of this may also have to do with the fact that phones are getting bigger (and thus more apparent to would-be-thief passersby): global shipments of smartphones with screens over 5 inches more than doubled from 25.6 million in 2012 to 60.4 million in 2013.[71]

The latter point is also somewhat reflected in the available data: according to a recent survey by the mobile security firm Lookout, 44% of phones are stolen because they are left behind in a public setting.[72] Though it may be possible that thieves are purposefully staking out public places like restaurants, clubs, or workplaces (the three most common places for phone theft to occur),[73] much of the rise in theft may simply be attributable to growing owner forgetfulness that comes along with increased smartphone usage in public. The fact that the average victim takes an entire hour to realize a theft[74] probably indicates that most stolen phones are not quickly swiped

---

Philadelphia, Seattle, Oakland, Long Beach, Newark, Detroit, Cleveland, Baltimore, New York, and Boston); *Phone Theft in America*, LOOKOUT MOBILE SECURITY (May 7, 2014), https://www.lookout.com/resources/reports/ phone-theft-in-america (noting that 55% of thefts occur in urban areas).

[70] *Device Ownership over Time*, PEW RESEARCH INTERNET PROJECT (accessed June 2, 2014), http://www.pewinternet.org/data-trend/mobile/device-ownership/.

[71] *Global Shipment of Smartphones with a Screen Size of 5 Inches or Larger*, STATISTA (accessed June 2, 2014), http://www.statista.com/statistics/253350/shipments-of-smartphones-with-screen-size-5-inches-or-larger/.

[72] *Phone Theft in America*, LOOKOUT MOBILE SECURITY (May 7, 2014), https://www.lookout.com/resources/reports/ phone-theft-in-america.

[73] *Id.*

[74] *Id.*

from right under the owner's nose. More likely, a restaurant or club patron leaves her phone on a table and another patron (or an employee) snatches it after the owner has left. If these circumstances are more likely to occur than specific targeting by thieves, then kill switches may not have their intended deterrent effect since many thieves seem to not calculate the risks of a theft ahead of time.

2. THIEVES MAY NOT LEARN ABOUT KILL SWITCHES OR EVEN CARE ABOUT STOLEN PHONE OPERABILITY

Even assuming that thieves engage in a risk calculus before attempting a theft, they may ignore the presence of a kill switch because they either do not know it exists or they do not care. It is often so easy to steal a smartphone that a thief may not mind the probability that he will be stuck with a bricked device. Thieves' opportunism not only takes advantage of the fact that "people on phones can be so oblivious to surroundings they are not aware of a potential thief"[75] but also of the 44 % of thefts that occur when phones are left behind in public settings. In these cases, taking a kill-switch-enabled phone presents little risk if the thief avoids getting caught, which most often is independent of the presence of a kill switch. If the phone is disabled, thieves may simply discard it and seek to steal another one.

Thieves also have another option. An inoperative smartphone can still retain some resale value, even if only for parts. Smartphone OS consultants and developers have suggested that components like the camera or the screen could fetch a price making it worthwhile to steal, while a thief could even damage a stolen smartphone and then claim the lower price that gadget recycling sites pay for broken hardware.

Would publicity about the mandatory deployment of kill switches in smartphones create a powerful enough deterrent for thieves? That depends on a number of

---

[75] Pegoraro, *supra* note 32 (internal citations omitted).

factors, such as (1) whether thieves would find out about kill switches personally, or through their fences; (2) how long would it take for theft to decrease once kill switches are deployed, which in turns depends on how long older versions of smartphones and OSs remain in use with consumers after the July 1, 2015 deadline; and (3) what thieves are stealing smartphones for.

The first factor above is at the center of a debate between state legislators trying to enact kill switch bills and manufacturers of security systems. While legislators want to publicize the deployment of kill switches to deter theft, security companies such as Absolute (the creator of the LoJack)[76] want unwitting thieves to continue connecting to the internet and cellular towers so that the company may track the thieves and gain remote access to stolen smartphones.

The third factor above is related to whether smartphone theft is targeted more at sensitive data than at the hardware itself. While a stolen smartphone may fetch a thief a few hundred dollars, access to financial apps, even for a short period of time, may be far more valuable.

What thieves are targeting ties into kill switch technical design choices as well. A software kill switch could protect a phone from getting wiped and reset, but it would not protect sensitive data encrypted on the smartphone. A hardware kill switch would be more secure, as described in Part V. However, while it would protect encrypted personal data, it could make it possible for thieves to reactivate the phone for resale. "We need to understand what the motivation is in the theft before instilling a solution," says Greg Kazmierczak, CTO of Wave Systems, a provider of hardware-based encryption technology, "What's the most valuable component — the hardware or the data you are storing in your device?"[77]

---

[76] Absolute, *supra* note 44.

[77] Jane Porter, *Is a Mandatory Kill Switch the Solution to Smartphone Theft?*, FORTUNE (May 27, 2014, 7:26 PM), http://fortune.com/2014/05/27/is-a-mandatory-kill-switch-the-solution-to-smartphone-theft.

3. THIEVES MAY TRUST THE BLACK MARKET TO END-RUN AROUND THE KILL SWITCH

Thieves, even if they learn of and care about the effectiveness of kill switches, may still steal because they have access to workarounds or are willing to wait for them. In Washington, D.C., a spokesman for the Metro transit system, Dan Stessel, pointed out that some stolen smartphones could be resold through buy-back programs like ecoATM kiosks that do not require face-to-face transactions.[78] ecoATM responded with a statement: "Our policy is not to knowingly purchase phones with Find My iPhone activated, and we continue to improve our technology to that end."[79]

Even if no mechanism for resale is available at the time of theft, thieves may still impute some expected value from the stolen phone by sitting and waiting for a hack or new distribution stream. This is precisely what happened with the doulCi hack mentioned above in Part V(B), where pictures of groups of newly jailbroken iPhones appeared on social media the day the hack was publicized. The hackers posted server data corroborating claims that "more than 5,700 devices [were hacked] in just five minutes."[80] Precedents like these encourage thieves that "brickable" phones may still be worth stealing, so long as waiting for a value-adding hack to come along is possible. The assumptions in this section highlight the uncertain effect a kill switch may have at deterring theft, if it even has an effect at all.

B. WHAT MINIMUM LEVEL OF KILL SWITCH TECHNOLOGY WOULD SUFFICIENTLY DETER THEFT?

As discussed in Part V, a kill switch would be less vulnerable to hacking or jailbreaking, as its level of implementation gets lower. For higher levels of implementation in software, a thief could jailbreak the

---

[78] *Id.*
[79] *Id.*
[80] Heath, *supra* note 39.

smartphone (done today for security apps installed on top of the OS), replace the OS, edit the BIOS file, or wipe the IMEI number (listed with increasing levels of difficulty and therefore increasing levels of deterrence to theft). To be more secure, a kill switch should be implemented at a lower level or directly in hardware. However, the lower the level of implementation and more secure the kill switch, the more expensive it will be to design and implement for manufacturers.

1. IN SEARCH OF AN OPTIMAL KILL SWITCH SOLUTION

Designing the best kill switch is an optimization problem: what is the minimum level of kill switch technology needed that will prove enough of a deterrence to a thief? The most expensive military-style solutions may not be needed as long as there is a sufficient deterrence to reduce theft by a desired amount. As with most optimization problems, an optimal solution would depend on the value of the inputs and ensuring the correct inputs have been chosen. It is hard to predict what factors of a kill switch would be optimal. In Figure 1, we illustrate an example graphical representation of theft deterrence versus kill switch technology, showing how the cost of a kill switch and the cost of cracking it could lead to an optimal solution.

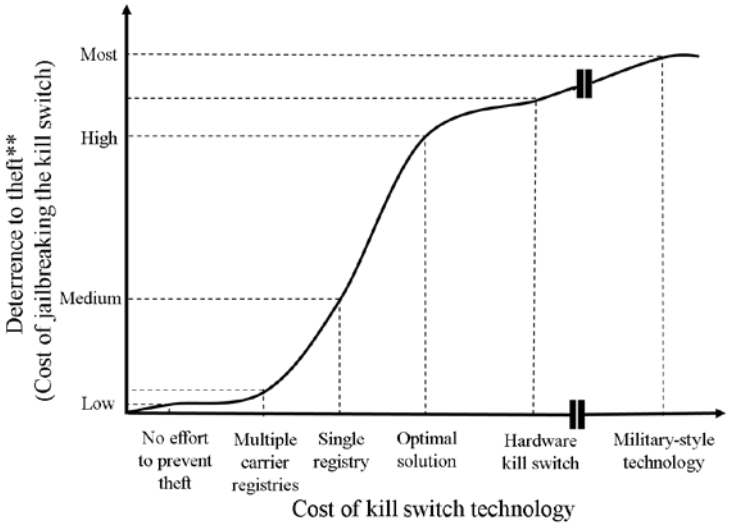

Figure 1. Illustration of the potential relationship between kill switch technology and levels of theft deterrence.

Making no special effort has little to no theft deterrence. Multiple carrier registries for difference carriers and different wireless standards (CDMA, GSM, and LTE) that carriers must only voluntarily consult provides a slightly higher level of deterrence. Using a single, shared carrier registry that carriers may be required to use to block stolen IMEI numbers by law, as in the case of Australia's EMTA, provides an even higher level of theft deterrence. Mandating the most secure (and expensive) military-style solution, such as the Boeing black phone, may provide the maximum possible level of theft deterrence. However, the expense of implementing it may not be commercially feasible: a cheaper hardware implementation alternative may be provide nearly as much deterrence at a far-reduced cost. The optimal solution may be a mixed software/hardware implementation at the knee of the curve that provides a high level amount of theft deterrence at a cheaper cost.

2. A SIMPLISTIC MODEL OF THEFT BEHAVIOR

An empirical study on theft deterrence versus kill switch technologies that takes into account factors such as the notice of a kill switch to thieves, the amount of implementation cost that industry is willing to absorb if mandated by law, and the cost of jailbreaking each level of kill switch technology would be useful to flesh out what an optimal solution may look like. Finally, a study on whether smartphone thieves are rational actors would be useful. This is because models such as the one illustrated above operate on a number of assumptions that may be incorrect. The following simplified model of thieving behavior demonstrates that—assuming thieves are rational actors—much is unknown about why thefts occur. If a kill switch solution misunderstands the reason for theft, it may prove costly and ineffective. For example, a thief's decision in deciding to steal a smartphone can be represented by the following equation.

$$\text{Steal if: } \mathrm{U}[\mathrm{E}(phone)] > U[|E(caught)|],$$

where U represents utility, E(*phone*) represents the expected value of the stolen smartphone, and E(caught) represents the expected value of getting caught. U[E(*phone*)] may be calculated as follows.

$$\begin{aligned}\mathrm{U}[\mathrm{E}(phone)] = \{&[1 - p(no\ catch, kill\ switch) - p(caught)] \\ &* E[profit(fence\ phone)]\} \\ &+ \{[p(no\ catch, kill\ switch) - p\ (caught)] \\ &* E[profit(sell\ parts)]\} + \beta,\end{aligned}$$

where β represents any extraneous positive or negative utility (over the sale value) that a thief gets from successfully stealing and selling a phone. Further, U[| E(*caught*) |] may be calculated as follows.

$$\mathrm{U}[|E(caught)|] = EU(caught) = p(caught) * |E(caught)|$$

If we assume a 15% catch rate of thieves and a 75% probability of a thief evading capture and encountering an unbreakable kill switch, we have the following incentive structure:

$$\mathrm{U}[\mathrm{E}(phone)] = (.1)^* E[profit(fence\ phone)] + (.6)^* E[profit(sell\ parts)] + \beta.$$

To continue working through the simplified model, assume a thief can net $200 profit on average for fencing a jailbroken phone and a $100 profit on average from either

selling the parts on a kill-switch-enabled phone or (if available) paying a hacker to bypass the kill switch. A thief can expect:

$$U[E(phone)] = 80 + \beta;$$

Steal if : $80 + \beta > EU(caught)$

A rational thief will therefore steal the phone so long as the expected value of stealing a phone (here, $80 + \beta$) exceeds the expected value loss from being caught. Assuming that β is nominal and the probability of being caught remains 15%, a rational thief will steal a phone unless his expected value loss from being caught is greater than roughly $533:

$$(.15) * E(caught) \geq 80,$$
$$or\ Steal\ unless: |E(caught)| \geq \approx 533$$

To take it a step further, even assuming that a thief has a 100% chance of either being caught or encountering a kill switch (say, $p(caught) = .15$ and $p(no\ catch, kill\ switch) = .85$), the thief may still gain utility from selling the parts or awaiting a hack to bypass the switch:

$$U[E(phone)] = (0)^* 200 + (.7)^* 100 + \beta = 70 + \beta;$$
$$Steal\ if: 70 + \beta > EU(caught);$$
$$(.15) * E(caught) \geq 70,$$
$$or\ Steal\ unless: |E(caught)| \geq \approx 467$$

Thus, a rational thief who fully comprehends the existence and effect of a kill switch ubiquitous on all phones could still decide to steal a phone, if only to make a profit off of selling hardware or data on the black market.

Clearly, this exercise does not purport to represent the reality of thieving behavior, but rather to show how difficult it is to understand the rationale behind stealing a phone. An endless number of additional assumptions can be introduced to the model (such as a negative effect on utility when encountering a kill-switch-enabled phone to represent confusion), and the model still remains a gross oversimplification of reality. The core assumption that thieves are rational actors is also incredibly dubious. Most phone thieves probably won't bother to calculate a detailed incentives equation like the one above, and thus they may not respond well to changing incentives (like the introduction of kill switches).

C. COULD VIGILANTISM HURT THE KILL SWITCH'S SAFETY OBJECTIVE?

The stated objective of both the SOS initiative and the various kill switch bills in state legislatures is to increase consumer safety by preventing (violent) theft. However, only 11% of smartphone theft involves a robber taking a smartphone from a person.[81] Moreover, 68% of theft victims reported a willingness to resort to vigilantism to recover their smartphones.[82] New apps such as Find My iPhone offer GPS tracking capabilities for those desperate to recover their smartphones, stirring worries among law enforcement officials that people are putting themselves and others in danger.[83] "Some have been successful," said George Gascón, the San Francisco district attorney and a former police chief, "others have gotten hurt."[84]

Pursuing a thief can lead to violence, especially when people arm themselves—hammers are popular—while hunting for stolen smartphones. A New Jersey man was arrested after he tracked his stolen smartphone and ended up attacking the wrong man, mistaking him for the thief.[85]

A kill switch could lead to increased violence in three ways. First, the way in which it is implemented could make it easier to track a stolen smartphone and take the law into one's own hands. Second, a thief who knows that an owner can brick a stolen smartphone may violently attack the owner during the robbery to prevent the owner from recovering and "bricking" the stolen smartphone too

---

[81] LOOKOUT, *supra* note5.
[82] *Id.*
[83] Ian Lovett, *When Hitting 'Find My iPhone' Takes You to a Thief's Doorstep*, N.Y. TIMES (May 3, 2014), *available at* http://www.nytimes.com/2014/05/04/us/when-hitting-find-my-iphone-takes-you-to-a-thiefs-doorstep.html.
[84] *Id.*
[85] *Id.*

soon. Third, if the "bricked" smartphone displays the owner's address, as some security apps and MDM solutions do, that could invite retribution from a frustrated thief.[86] Further investigation of whether a kill switch implementation would increase vigilantism and violence above the level already occurring with apps such as Find My iPhone is critical before defining a kill switch standard and settling on a particular implementation.

However, vigilantism is also fueled by the dismissive responses that victims of theft receive from manufacturers and service carriers. For example, a victim who tracked his stolen smartphone to a particular house and called AT&T was given two options by the carrier: either deactivate the phone and buy a new one, or find a cop willing to subpoena AT&T for information, file a lengthy police report, and go through a long bureaucratic process.[87] Manufacturers and carriers have little incentive to help a victim recover a device because the manufacturer profits by hawking a replacement phone; and the carrier profits by locking the crime victim into a new contract, then opening an account with whomever ends up with the stolen phone.[88] Carriers even profit from the specter of phone theft, by selling expensive insurance policies to protect their users. A mandatory kill switch could reverse this trend and potentially reverse the need for vigilantism by turning stolen smartphones worthless or promoting their recovery.

D. EXEMPT DEVICES COULD REDUCE THEFT DETERRENCE

As we describe in Part V, the millions of older versions of smartphones still in use by the deployment deadline would defeat the theft deterrence objective of the kill switch legislation by around two years. In addition, the presence of other exempt devices would also drag the level of deterrence downward. For example, the California

---

[86] MORLEY, *supra* note 68.
[87] Swan, *supra* note 17.
[88] *Id.*

Senate Energy, Utilities, and Communication Committee listed the following exempt devices that would not be required to have a kill switch.

> All devices that fall within the exception for resale and pawnbrokers; All devices sold out of state and brought into California; All devices currently in the market, which customers typically replace every 18 to 24 months; All devices provided "free" as part of a promotion or a wireless lifeline plan; and All devices that, even if rendered inoperable by a kill switch, may have value for parts.[89]

Such devices would continue to have value for resale on the black market. Moreover, the potentially large number of such devices in use would incentivize thieves to take their chances with a kill switch and continue with smartphone theft.

E. The Power of Default

The various pieces of legislation mandating a kill switch for smartphones have provisions stating that each smartphone sold must have the kill switch enabled but that consumers should have the ability to disable the kill switch upon purchase. On the other hand, the CTIA and third-party security app vendors such as Absolute would prefer that any kill switch be deployed on an opt-in basis, with consumers choosing whether to opt in to the program. While an opt-in program puts consumer choice front and center in deciding how a kill switch would be deployed, the choice of whether a kill switch program is

---

[89] California Senate, Energy, Utilities and Communications Committee, March 24, 2014, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB962&search_keywords (click Bill Analysis tab, then click the link titled "03/28/14 – Senate, Utilities And Communications").

opt-in or opt-out will have a significant impact of whether kill switches will be adopted by the majority of smartphone owners.

The choice of the default position is based on three assumptions from behavioral economics. First, more consumers stay with the default than would choose to do so if forced to choose.[90] Second, only consumers who prefer the opt-out choice will opt out. And third, where carriers oppose the default position, they will be forced to explain it to smartphone owners, resulting in well-informed decisions by consumers. However, Professor Willis asserts, in the privacy context, that these assumptions are unlikely to hold.

The default position, such as an opt-in kill switch, favored by companies is often surrounded by a powerful campaign to keep consumers there, but a default position set contrary to company interests can be met with an equally powerful campaign to drive consumers out.[91] Therefore, companies can either bolster the mechanisms behind the inertia that leads consumers to stick with defaults or they can weaken them to induce consumers to opt out. Rather than forcing companies to facilitate consumer exercise of informed choice, many defaults leave companies with opportunities to play on consumer biases or confuse consumers into sticking with or opting out of the default.[92] However, to really deter theft, smartphones will require near–100 % adoption, such that thieves stop taking the chance that a given smartphone will have the kill switch disabled.

F. TRACKING LOCAL SMARTPHONE SALES AND INCREASED PENALTIES FOR IMEI WIPING

In 2013, New York State Senate Co-Leader Jeffrey Klein and Assemblyman Jeff Dinowitz, Chair of the Assembly's Consumer Affairs and Protection Committee,

---

[90] Lauren E. Willis, *Why Not Privacy By Default?*, 29 BERKELEY TECH. L.J. 61 (forthcoming 2014).
[91] *Id.*
[92] *Id.*.

introduced new legislation to require smartphone sellers to prove that they are the rightful owners of the phones they sell.[93] The objective of the legislation is to curtail the local black market for stolen smartphones. Non-compliant sellers face the possibility of steep fines or jail time.[94] The state lawmakers hope that this legislation would stop stolen smartphones being sold at neighborhood stores, laundromats, and flea market stands.

The legislation would require smartphone sellers to provide detailed receipts for every phone sold, including the IMEI number. It is hoped that these records could provide additional information on how and where stolen phones move in the marketplace. However, Arieanna Schweber of Absolute Software claims that although the bill could make the sale of stolen mobile phones locally more difficult, it will not diminish the demand for stolen devices.[95] This is because the majority of stolen smartphones are now being shipped abroad. Therefore, local legislation will likely be inadequate to address the global issue.

Also in 2013, U.S. Senator Charles E. Schumer reintroduced legislation that would make it a federal crime to wipe an IMEI number by imposing a five-year criminal penalty.[96] Senator Schumer noted that without a criminal penalty for tampering with IMEI numbers, thieves could simply alter the IMEI number to evade carrier registries and reactivate a smartphone phone. Because the bill has the full support of the CTIA and the FCC, it could prevent reactivation of stolen smartphones. However, it may have little deterrence value if smartphones are primarily being stolen for an international black market.

---

[93] S. 5976, 2013 Leg., Reg. Sess. (N.Y. 2013).

[94] *See, e.g.*, CAL. BUS. & PROF. CODE § 22761(c) (West 2014) ("The knowing retail sale of a smartphone in California . . . may be subject to a civil penalty").

[95] Arieanna Schweber, *New York Legislators Propose Law to Reduce Black Market for Mobile Devices*, INTELLIGENCE (Oct. 21, 2013), http://theft319.rssing.com/browser.php?indx=16105444&item=24.

[96] S. 1070, 112th Cong. (2013).

VII. ADDITIONAL CONCERNS AND PRACTICAL DIFFICULTIES OF A MANDATORY KILL SWITCH

A government-mandated kill switch, as opposed to allowing individuals to make their own security choices, raises several additional concerns and risks of misuse and surveillance.

A. GOVERNMENT SURVEILLANCE AND CONTROL

Although Internet companies and government agencies already track bulk and targeted data on the Internet, individuals today have the ability to erase and block tracking cookies, prevent the transmission of specified local data, and even use encryption technology, given enough technical savvy.[97] However, mandatory phone kill switches have the potential to significantly increase government surveillance and control over speech and political behavior. On August 11, 2011, the Bay Area Rapid Transit system (BART) shut down cellphone service to four stations in San Francisco in response to a planned protest, because in July 2011 protesters disrupted BART service in response to the fatal shooting of a passenger by BART police.[98] BART first approached carriers directly and asked them to turn off service. Later, a BART officer asserted that "BART staff or contractors shut down power to the nodes and alerted the cell carriers" after the fact.[99] A smartphone kill switch that the government can control by exerting authority over carriers could even more greatly empower the government to squelch political protests by disrupting smartphone service and making organization

---

[97] Thomas Claburn, *Kill Switches: Phones Just the Start*, INFORMATIONWEEK (Feb. 19, 2014, 9:06 AM), http://www.informationweek.com/mobile/mobile-devices/kill-switches-phones-just-the-start/d/d-id/1113887.

[98] Eva Galperin, *BART Pulls a Mubarak in San Francisco*, ELECTRONIC FRONTIER FOUNDATION (Aug. 12, 2011), https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco.

[99] *Id.* (quoting James Allison, deputy chief communications officer for BART).

and coordination of citizen movements or protests difficult.

The Electronic Frontier Foundation (EFF) compared BART's actions with those of former President Hosni Mubarak of Egypt who ordered the shutdown of cellphone service in Tahrir Square in response to peaceful, democratic protests in 2011.[100] Moreover, British Prime Minister David Cameron is considering new, broad censorship powers over social networks, such as Facebook and Twitter and mobile communication in the UK.[101] The ability to peremptorily control smartphone kill switches could have grave concerns for free speech and democracy. However, BART was able to shut down cellphones without a kill switch. Therefore, whether kill switches really represent a broad enlargement of the government's power requires information on how much a kill switch would add to the government's current ability to turn off smartphone communications. The advantage of a kill switch that the government has the ability to control is that it could prevent theft of trade secrets and national secrets from stolen smartphones. Further study would be welcome on how this would work with or without the consent of the smartphone's owner.

B. INSECURE NON-OWNER CONTROL

As the CTIA points out, even if a kill switch is technologically feasible, it could have serious risks. If a mandatory kill switch is created, every smartphone would have the capability. Depending on the implementation, the "kill" message could be known to every operator and could not be kept secret.[102] A private party with malicious

---

[100] *Id.*

[101] James Kirkup, *UK Riots: Tougher Powers Could Curb Twitter*, THE TELEGRAPH (Aug. 12, 2011, 8:20 AM), http://www.telegraph.co.uk/news/uknews/crime/8697142/UK-riots-tougher-powers-could-curb-Twitter.html.

[102] CTIA, *Why a "Kill Switch" Isn't the Answer*, http://files.ctia.org/pdf/Why_a_Kill_Switch_Isn_t_the_Answer.pdf.

intent could therefore replicate the "kill" message, such as a text or other message sent to the smartphone to disable it. In another scenario, if "killing" a smartphone requires a call to the carrier, that call could be placed by an identity theft who does not possess the smartphone or an abusive spouse who actually owns the family account to which his wife's smartphone is tied. Where a smartphone is disabled by the malicious use of a "kill switch," the safety of the user may be jeopardized, as in the abusive spouse scenario, because the wife will be unable to make emergency calls.

By sending multiple messages, such as by incrementing the telephone number or IMEI number, groups of smartphones could be disabled. This could be used to disable entire groups of customers, such as the Department of Defense, the Department of Homeland Security or emergency services and law enforcement.[103] If the kill switch is a permanent switch, a smartphone could be disabled forever. The risk of denial of service could be far too large. Therefore, the carrier community maintains that control of operation (and denial of service) be embedded in the network and not at the smartphone-level.[104]

C. FARADAY BAG WORKAROUNDS

Driven by high prices for non-contract smartphones overseas, the underground trade of stolen smartphones has now become a global enterprise that connects violent street thieves in American cities with buyers as far away as Hong Kong, according to law enforcement and the wireless industry. Jerry Deaven, an agent with the Department of Homeland Security, which is tasked with preventing the trafficking of stolen goods, told The Huffington Post that traffickers are responsible for "a tremendous amount of phones being shipped out of the country," adding that "some organizations are shipping a

---

[103] *Id.*
[104] *Id.*

couple million dollars worth of phones per month."[105] Some stolen smartphones are placed into Faraday Bags immediately after being stolen to block GPS tracking. Further study is required on whether a Faraday Bag could be used to circumvent a kill switch, and, if so, whether a smartphone stolen in the U.S. could then be activated abroad. How about a stolen smartphone with a "kill switch" taken from California in a Faraday Bag to Arizona or Nevada, states without corresponding kill switch legislation. Ultimately the answers to these questions will help determine whether a kill switch would be a better solution than carrier registries, and, if so, help drive the design of an optimal kill switch.

D. MINIMIZING THE BURDEN ON SMARTPHONE OWNERS

Finally, the amount of user effort needed to deal with kill switch systems, including notifying carriers in the event of theft or loss, reversing the data wipe and "un-bricking" a smartphone after recovery, or heading off the kill command in the event a misplaced smartphone is found, should not burden smartphone owners in the same way passwords do. For example, computer users today are required or strongly encouraged to employ different, long, and complicated passwords on each of multiple devices: laptops, tablets, desktops; and multiple accounts: financial websites, health websites, company logins, Google, etc.[106]

The Office of California Attorney General Kamala Harris advises users and businesses on computer security,

---

[105] Gerry Smith, *Inside the Massive Global Black Market for Smartphones*, HUFFINGTON POST (July 13, 2013, 2:56 PM), http://www.huffingtonpost.com/2013/07/13/smartphone-black-market_n_3510341.html?utm_hp_ref=iphone-theft.

[106] Chenda Ngak, *The 25 Most Common Passwords of 2013*, CBS NEWS (Jan. 21, 2014, 11:14 AM), http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013 ("[T]he top three passwords of [2013] are '123456,' 'password' and '12345678'.").

including using firewalls, anti-virus software, and complex passwords.[107] However, passwords have done little to prevent hacking of sensitive information and cyber-attacks. California businesses and the government have experienced 300 separate data breaches exposing the personal information of more than 20 million customer accounts during the past two years.[108] Complex password requirements therefore simply burden users without actually preventing hacking. Any proposed kill switch technology and carrier response protocols should be designed to minimize the burden on users while burdening smartphone thieves instead. A study on the lessons the industry or analysts have learned from the failed decades-long password experiment would be useful to prevent repeating this costly mistake on smartphone kill switches.

VIII. EFFECTIVENESS OF STATE LEGISLATIVE APPROACHES: PATCHWORK REGULATION IN A NATIONAL / INTERNATIONAL MARKETPLACE

The decentralized nature of the mandatory kill switch movement presents a host of concerns for proper implementation of an effective and democratic solution. The practical reality of state-by-state piecemeal legislation is that the bigger, more influential states tend to drive policy. Thus, while Minnesota has passed its kill switch legislation and gained a first mover's advantage, pragmatically the bill only applies to phones sold or purchased new in Minnesota. This is not to say that threats of foreclosing a state market will have no effect on phone providers—risking infringement of the Minnesota

---

[107] State of California, Office of the Attorney General, *Is Your Computer Secure?*, http://oag.ca.gov/privacy/facts/online-privacy/computer-secure.

[108] Don Thompson, California to Step Up Cybersecurity Efforts After Hundreds of DatauBreaches, SAN JOSE MERCURY NEWS (Feb. 27, 2014, 10:26 AM), http://www.mercurynews.com/business/ci_25240431/california-step-up-cybersecurity-efforts-after-hundreds-data.

bill may encourage all phone manufacturers and carriers to comply with the kill switch mandate. However, patchwork state mandates of kill switches may do little to deter thieves, particularly where there is doubt over where the phone was bought.

The real test of the legislation's viability (and the site of potential legal challenges) however arises in the larger states where more phones are sold. Hence, California and New York are the likely battlegrounds for policy development and industry regulation. Because roughly one-eighth of all Americans live in California, and Apple and Google are based there, the California law may very well produce an immediate national default.[109]

This potential California effect risks legislating national policy at the state level and may very well overstep the ability of other democratically elected leaders to have a say in how kill switches should be adopted, if they should at all. The CTIA claims, for instance, that the Minnesota bill creates interstate commerce concerns "because it heavily burdens the national wireless device and service market by dictating operational and technical specifications of mobile devices."[110] At the same time, coordinating state legislation is potentially challenging, unnecessary, and time-consuming. According to the Secure Our Smartphones initiative, twenty-three state Attorneys General support the proposal, among many

---

[109] Wagenseil, *supra* note 16. *See also* Elizabeth Weise, *Google, Microsoft to add "kill switches" to phones*, USA Today (June 20, 2014, 3:11 PM), http://www.usatoday.com/story/tech/2014/06/20/google-microsoft-kill-switches/11083511/.

[110] Jamie Hastings, Vice President of External & State Affairs, CTIA—The Wireless Association, Testimony in Opposition to Minnesota House File 1952, Minnesota House Commerce and Consumer Protection Finance and Policy Committee, March 19, 2014, http://www.ctia.org/docs/default-source/Legislative-Activity/ctia-testimony-in-opposition-to-minnesota-house-file-1952-requiring-kill-switches-on-mobile-devices.pdf?sfvrsn=0.

other district attorneys and other state political figures.[111] Many of these states whose attorneys general support a mandatory kill switch may simply prefer to conserve political resources and allow other states, like California, to drive the policy. Kill switch opponents, however, will then likely argue that such a proposal has no opportunity to be debated by democratically elected state representatives, who may have valuable input on the matter. In truth, kill switch bills are not passing legislatures easily. There are only five state bills and one federal bill passed or pending, and California's version was rejected once in the state senate before narrowly passing recently.[112] The federal kill switch bill, which would pose fewer of the risks that accompany state piecemeal legislation, has experienced little movement since being announced in February 2014.

Technological mandates in general are difficult to accomplish successfully by government legislation, much less state-by-state legislation. As the CTIA explains, there is little reason to "limit consumer choice by mandating the use of any solution . . . [because] [a]ny mandated technology standard will quickly become outdated in the fast-moving world of wireless applications and technology."[113] The private sector's hesitance to accept government technology mandates is not unreasonable, particularly in a sector of rapid innovation like mobile phones. Politicians, many of whom have little technical comprehension of the issue, are likely not the ideal decision-makers on how technology must be used.

Nonetheless, there is a fitting example of an effective technological mandate on a similar issue as the smartphone kill switch. Car theft laws, passed in the 1980s and 1990s, successfully decreased auto theft by increasing

---

[111] Secure Our Smartphone Initiative Members, Office of New York Attorney General Eric T. Schneiderman, http://www.ag.ny.gov/sos/initiative-members.
[112] Chloe Albanesius, *California State Senate Rejects Smartphone Kill-Switch Bill*, PC MAGAZINE (April 25, 2014, 10:35 AM), http://www.pcmag.com/article2/0,2817,2457117,00.asp.
[113] Jamie Hastings, *supra* note 110.

penalties for thieves and mandating implementation of anti-theft vehicle identification numbers on the engine, transmission, and other main body parts (which became illegal to remove).[114] This movement, however, was aided in large part by federal legislation, namely the 1984 Motor Vehicle Theft Law Enforcement Act, which federally implemented the above, and the 1994 Motor Vehicle Theft Prevention Act, which mandated federal cooperation with states to create an opt-in program whereby volunteers would consent to law enforcement stopping the car if it were operated in certain conditions (such as late at night).[115] Further, the anti-auto-theft movement had federal oversight of exported cars to check for owner vehicle identification numbers.[116]

Clearly, no such solution is viable for smartphones, which are smaller and harder to track. While no authoritative data exists on this point, the international black market certainly provides an integral boon to smartphone theft. Especially in countries where smartphones are not widely imported, stolen phones can sell for incredibly high amounts that only reinforce the motive to internationally traffic stolen phones. In March 2013, California charged two men with operating a stolen phone trafficking ring to Hong Kong from which they made over $4 million in a year.[117] Another man being charged reportedly bought iPhones from people at coffee shops for $250 to $350 and trafficked them on his person to Vietnam, eleven at a time, making trips as often as he could, apparently making enough profit to justify the

---

[114] National Auto Auction Association, *History of Auto Theft Legislation: Federal Legislation*, (accessed June 5, 2014), http://www.naaa.com/NAAA_Legislative/history_auto-theft.html.

[115] *Id.*

[116] *Id.* (under the 1984 Motor Vehicle Theft Law Enforcement Act).

[117] Gerry Smith, *Inside the Massive Global Black Market for Smartphones*, Huffington Post (July 13, 2013, 2:56 PM), http://www.huffingtonpost.com/2013/07/13/smartphone-black-market_n_3510341.html.

trips.[118] Anecdotes such as these highlight the limits with even a comprehensive federal regulation aimed at deterring smartphone theft. A patchwork approach of kill switch mandates risks exploitation by both inter-state limitations and international black market workarounds. Mandatory kill switches, regardless of how effective they may seem, face many roadblocks to attaining their stated goal of deterring theft.

IX. CONCLUSIONS AND A CONCISE LIST OF OPEN QUESTIONS

As we have shown in this paper, the stakeholders in the kill switch debate, including legislators, smartphone manufacturers, and carriers are each operating on the basis of a large number of assumptions and unknowns, including the following:

- What an optimal technical implementation of a kill switch at no additional cost to the consumer would be, including whether it should be implemented in software, hardware, or an automated form of the present manual IMEI blocking registries;
- What role MDM solutions and carrier registries will play in or out of an environment in which kill switches are deployed;
- Whether the large increase in smartphone theft is because thieves are specially targeting smartphones or whether smartphone theft is only incidental or unrelated to typical robberies;
- Whether an effective kill switch will actually deter theft or only incentivize them to ship more stolen smartphones to the international black market; and
- Whether a kill switch presents concerns, such as government surveillance and malicious activation or circumvention.

In addition to the assumptions and unknowns above, there are significant practical concerns about

---

[118] *Id.*

actually implementing a kill switch at no cost to the consumer across varying industry smartphone platforms and operating systems by the legislation's deadline of July 1, 2015. A necessary first step to such an implementation would be for the wireless industry to properly define kill switch standards so each manufacturer could conform their hardware, operating systems, and design platform accordingly. The short runway presented by the state bills allows very little time for such standard-setting activity. Requiring a solution too soon may not consider the balance between (1) the nature, urgency and magnitude of the problem, and (2) the cost, harm to innovation, and burden on the wireless industry of any mandated change. For example, in discussing the possibility of adding a theft-resistant "kill switch" to future iPhone models, Apple noted that the next two generations of the iPhone have already been developed, and were designed before Steve Jobs's death in late 2011.[119] Therefore, the challenges of effectively implementing a technological mandate too quickly could be a significant burden on smartphone manufacturers to modify their planned pipeline of designs.

Developing sound policy to deter smartphone theft would therefore benefit from more in-depth investigation of smartphone theft psychology, the mechanics of the black market for smartphones, the merits of technological solutions, and how to most effectively implement an overall solution. The time for such investigation is now, as the landmark California legislation's mandate goes into effect on July 1, 2015.

APPENDIX: SELECTED TEXT OF LEGISLATIVE PROPOSALS

There are four state bills and one federal bill demanding mandatory kill switches: California S.B. 962; Minnesota H.B. 1952; Illinois S.B. 3539; New York A.B. 8984; and the federal Smartphone Theft Prevention Act,

---

[119] Daniel E. Dilger, *Apple Gov't Rep Says Next Two iPhones Were Designed Under Steve Jobs*, APPLEINSIDER (Apr. 1, 2013, 12:03 PM), http://appleinsider.com/articles/13/04/01/apple-govt-rep-says-next-two-iphones-were-designed-under-steve-jobs.

H.R. 4065. Minnesota's bill was signed into law on May 14, 2014, while California's bill passed the state senate on May 8, 2014 and became law on August 25, 2014. What follows is a brief description of key text from the bills.

California legislation S.B. 962 applies to smartphones manufactured and sold in California on or after July 1, 2015. It requires these smartphones to "[i]nclude a technological solution . . . [that] can render the essential features of the smartphone inoperable to an unauthorized user" (emphasis added). This technological solution "may consist of software, hardware, or a combination of both software and hardware." Here are some selected quotes from the bill, with underlines of key phrases:

- "The technological solution should be able to withstand a hard reset or operating system downgrade, come preequipped, and the default setting of the solution shall be to prompt the consumer to enable the solution during the initial device setup."
- "'Essential features' of a smartphone are the ability to use the device for voice communications, text messaging, and browse the Internet, including the ability to access and use mobile software applications."
- "The technological solution shall be reversible, so that if the rightful owner obtains possession of the device after the essential features of the smartphone have been rendered inoperable, the operation of those essential features can be restored by an authorized user."
- "An authorized user of a smartphone may affirmatively elect to disable or opt-out of enabling the technological solution at any time."
- "In order to be effective, antitheft technological solutions need to be ubiquitous, as thieves cannot distinguish between those smartphones that have the solutions enabled and those that do not."

- "The Legislature finds and declares that the enactment of a uniform policy to deter thefts of smartphones and to protect the privacy of smartphone users if their smartphones are involuntarily acquired by others is a matter of statewide concern."

Minnesota H.B. 1952, now passed as law, becomes effective on July 1, 2015 on all smartphones sold or purchased new in Minnesota. It provides that these smartphones "must be equipped with technology designed to render the device inoperable in the event of theft or loss." Here are some selected quotes from the bill:

- "Smart phone does not include an electronic reader, tablet, or other similar device not primarily intended for two-way voice communication."
- "[Must] be reversible in the event of the smart phone's recovery by its owner"
- "Lock all of the smart phone's user data, and ensure that it is only accessible to the user or a law enforcement officer subject to a valid search warrant"
- "Render the smart phone core functionality inoperable on any wireless telecommunications service provider's network globally"
- "Prevent the smart phone from being reactivated without a passcode or other similar authorization, even if the device is reprogrammed, is turned off and subsequently turned back on, has its network connectivity disabled and subsequently re-enabled, or has its SIM card removed"

New York's proposed A.B. 8984 (which did not make it out of the legislative committee) would be applicable to any advanced mobile communications device sold in New York on or after July 1, 2015, with "advanced mobile communications device" defined very similarly to California's definition with the exception of including

tablets. A.B. 8984's description of the kill switch functionality is also highly similar to California's, and its legislative intent tracks the rationale of California as well. The following two quotes are also of note:

- "It is the further intent of the legislature to prohibit any term or condition in a service contract between a customer and a commercial mobile radio service provider that requires or encourages the customer to disable the technological solution that renders the customer's smartphone or other advanced communications device useless if stolen."
- "The rightful owner of an advanced mobile communications device may affirmatively elect to disable the technological solution after sale. However, the physical acts necessary to disable to the technological solution may only be performed by the end-use consumer or a person specifically selected by the end-use consumer to disable the technological solution and shall not be physically performed by any retail seller of the advanced mobile communications device."

Illinois proposed S.B. 3539 (which did not make it out of the legislative committee) would apply immediately upon passage to any smartphones manufactured and sold in Illinois. S.B. 3539 is similar to the other legislation, but uniquely would require all violating providers to insure the phones at no cost to the consumer, rather than levying a per-phone monetary penalty. The following quotes are of note:

- "'Smartphone' means a cellular phone that is built on a mobile operating system and possesses advanced computing capability. Features a smart phone may possess include, but are not limited to, built-in applications, Internet access, digital voice service, text messaging, e-mail, and Internet browsing."

- "[P]ermanently remove all saved data on the device"
- "[R]ender the smart phone completely inoperable on any wireless telephone service provider's network, including a wireless telephone service provider's global network"
- "[P]revent the smart phone from being reactivated or reprogrammed without a password or other similar authorization"
- "[D]isable the device even if it is turned off or the SIM card or other data storage medium is removed"
- "[B]e reversible if the device is recovered by its owner."

The federal proposed Smartphone Theft Prevention Act, H.R. 4065, would have applied beginning January 1, 2015 on any mobile device manufactured in the U.S. or imported for sale to the public in the U.S. (it did not make it out of legislative committee). It would have covered any "'mobile device' [which] means a personal electronic device on which commercial mobile service or commercial mobile data service is provided" and included an exemption for any technology that "accomplishes the functional equivalent of the function" defined in the bill as being able to remotely and costlessly:

- "Delete or render inaccessible from the device all information relating to the account holder that has been placed on the device"
- "Render the device inoperable on the network of any provider of commercial mobile service or commercial mobile data service globally, even if the device is turned off or has the data storage medium removed"
- "Prevent the device from being reactivated or reprogrammed without a passcode or similar authorization after the device has been rendered inoperable or subject to an unauthorized factory reset"

- "[R]everse any action . . . if the device is recovered by the account holder."

In response to these pieces of legislation, the CTIA has produced its own voluntary opt-in commitment for carriers and manufacturers. The main provisions are as follows:

- Remote wipe the authorized user's data that is on the smartphone in the event it is lost or stolen.
- Render the smartphone inoperable to an unauthorized user (e.g., locking the smartphone so it cannot be used without a password or PIN), except in accordance with FCC rules for 911 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., "phone home").
- Prevent reactivation without authorized user's permission (including unauthorized factory reset attempts) to the extent technologically feasible
- Reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible (e.g., restored from the cloud).