McGeorge Law Review

Volume 46 | Issue 2 Article 2

1-1-2014

Chapter 275: The Fight to Protect Consumers with a Kill Switch May Leave Them Tone Deaf

Jenifer Gee
Pacific McGeorge School of Law

Chapter 275: The Fight to Protect Consumers with a Kill Switch May Leave Them Tone Deaf

Jenifer Gee

Code Section Affected:
Business and Professions Code § 22761 (new).
SB 962 (Leno); 2014 STAT. Ch. 275.

TABLE OF CONTENTS

I. INTRODUCTION

Smartphone[1] thefts are a growing criminal trend in major cities.[2] For example, in 2012, the number of stolen smartphones in San Francisco accounted

1. Smartphones are defined as mobile devices that can search the Internet, run applications, send and receive text messages and email, and have voice communication capabilities. CAL. BUS. & PROF. CODE §22761(a)(1)(A)(i)-(iv) (enacted by Chapter 275); *see also* BUS. & PROF. §22761(a)(1)(B) (enacted by Chapter 275) (stating for the purposes of Chapter 275, the term "smartphone" "does not include a radio cellular telephone," which is also referred to as a "messaging" phone, nor does it include a laptop, tablet or e-reader). The "'essential features' of a smartphone" include voice communications, Internet browsing, and access to applications. BUS. & PROF. §22761(a)(2) (enacted by Chapter 275).

2. Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, Secure Our Smartphones Initiative Statement (June 13, 2013), *available at* http://www.ag.ny.gov/sos/secure-our-smartphones-initiative-statement (on file with the *McGeorge Law Review*).

for 50% of the city's robberies.[3] In Los Angeles, police officials reported that the increasing rate of cellular phone and smartphone thefts made the devices the "second most commonly stolen item, after money."[4] In 2014, the San Francisco District Attorney's Office reported that smartphone thefts accounted for 65% of robberies in San Francisco and 75% of robberies in Oakland.[5]

The cost of smartphone thefts is both financial and, unfortunately in some cases, physical.[6] The Consumer Reports National Research Center found that national smartphone thefts almost doubled from 2012 to 2013, rising to 3.1 million thefts.[7] As new smartphones, such as the iPhone 6 Plus, can cost nearly $1,000, smartphone thefts impose a significant financial burden on consumers.[8] One study estimates that consumers nationwide spend $580 million per year replacing lost or stolen phones.[9] Beyond the financial loss, some smartphone thefts lead to violence.[10] In one incident, San Francisco Police reported that two men cut a tourist's face with knives while stealing his iPhone.[11]

Due to the rise in smartphone thefts and associated costs, Senator Leno introduced Chapter 275 to reduce smartphone-related crimes.[12]

II. LEGAL BACKGROUND

This section will explore the development of federal and state laws that purport to provide greater security for smartphone users.[13] In particular, this section will discuss early attempts to curb smartphone thefts,[14] examine proposed

---

3. *Id.*

4. Press Release, L.A. Police Dep't, Cellular phones Trending as Choice Loot for Thieves (Apr. 13, 2012), *available at* http://www.lapdonline.org/april_2012/news_view/50765 (on file with the *McGeorge Law Review*).

5. Press Release, S.F. Dist. Attorney, Smartphone Theft Prevention Act Clears First Committee Vote (Apr. 1, 2014), *available at* http://www.sfdistrictattorney.org/index.aspx?page=345 (on file with the *McGeorge Law Review*).

6. S.F. POLICE DEP'T, PERFORMANCE WITH A PURPOSE: 2012 ANNUAL REPORT 47 (2012), *available at* http://sf-police.org/index.aspx?page=3992 (on file with the *McGeorge Law Review*) (stating some victims are "accosted, slapped or pushed down" during the theft of a smartphone).

7. *Smart Phone Thefts Rose to 3.1 Million Last Year, Consumer Report Finds*, CONSUMER REPORTS, http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm (last updated May 28, 2014, 4:00 PM) (on file with the *McGeorge Law Review*).

8. *Shop iPhone 6 Plus*, APPLE INC., http://store.apple.com/us/buy-iphone/iphone6/5.5-inch-display-128gb-space-gray-unlocked (last visited Jan. 16, 2015) (advertising the iPhone 6 Plus for $949).

9. DR. WILLIAM DUCKWORTH, ANTI-THEFT SOFTWARE IN MOBILE PHONES COULD SAVE CONSUMERS $2.6B A YEAR, EXECUTIVE SUMMARY 2 (2014) (on file with the *McGeorge Law Review*).

10. S.F. POLICE DEP'T, *supra* note 6 at 47.

11. *Id.*

12. SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS, COMMITTEE ANALYSIS OF SB 962, at 3 (Mar. 24, 2014).

13. *Infra* Part II.A.

14. *Id.*

federal legislation,[15] and analyze California law that enables law enforcement to interrupt cellular phone service.[16]

A. Recent Attempts to Stop Thefts

In 2013, law enforcement and cellular phone companies joined forces to launch a national database for lost and stolen phones.[17] The database allows cellular phone providers to check whether a device has been reported missing or stolen before granting service to it.[18] If a consumer's phone is stolen, he or she must report the theft to law enforcement and the service provider to have the device added to the database.[19] Only law enforcement and wireless companies can access information in the database.[20]

Critics say the database is ineffective because thefts have continued to rise and thieves have found ways to gain unauthorized access to stolen phones and use them.[21] After the introduction of the database, those same critics advocated for a kill switch in smartphones to let consumers shut-off their phones and thwart entry into their devices.[22] A kill switch is a "technological solution that renders the essential features of the device inoperable when stolen."[23] A smartphone owner's activation of a kill switch allows the owner to "[r]ender the essential features of [the] device (voice and Internet service) inoperable . . . ; [and p]revent reactivation of the device on a wireless network except by the rightful owner."[24]

---

15. *Infra* Part II.B.

16. *Infra* Part II.C.

17. *FAQ on Lost/Stolen Devices*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/faq-on-lost-stolen-devices (last updated Apr. 2014) (on file with the *McGeorge Law Review*).

18. *Id.*

19. FED. COMMC'NS COMM'N, STOLEN AND LOST WIRELESS DEVICES 1–2, *available at* http://transition.fcc.gov/cgb/consumerfacts/lostwirelessdevices.pdf (2014) (on file with the *McGeorge Law Review*). Consumers need their account information or phone number to report a lost or stolen phone; for example, T-Mobile customers need to log-in online to their account to suspend service. *Report a Lost or Stolen Phone*, T-MOBILE, http://support.t-mobile.com/docs/DOC-1211 (last modified July 10, 2014, 8:05 AM) (on file with the *McGeorge Law Review*). AT&T customers can also log-in to suspend service or call the company and provide the phone number of the stolen device. *Replace Your Lost or Stolen Device and Suspend Service*, AT&T, http://www.att.com/esupport/article.jsp?sid=KB63935&cv=820# (last visited Sept. 10, 2014) (on file with the *McGeorge Law Review*). The success of the database is based on whether customers report their stolen phones. SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS, COMMITTEE ANALYSIS OF SB 962, at 2 (Mar. 24, 2014).

20. *FAQ on Lost/Stolen Devices*, *supra* note 17.

21. Press Release, N,Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2. Some smartphone thieves simply reactivate stolen phones while others use the phone after removing its SIM card. *Id.*

22. *See, e.g. id.* (calling for the implementation of a kill switch "now").

23. SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS, COMMITTEE ANALYSIS OF SB 962, at 3 (Mar. 24, 2014).

24. *Id.*

Supporters of a kill switch solution argue the database is ineffective, while database advocates argue more time is needed to assess the database's value.[25]

Critics of the database argue that consumers need more than a list of stolen phones to deter smartphone thefts.[26] In June 2013, the San Francisco District Attorney joined with the New York Attorney General to launch the Secure Our Smartphones Initiative (the Initiative).[27] The Initiative calls on smartphone manufacturers to install a kill switch in every device so its owner can render the unit inoperable if lost or stolen.[28]

In June 2014, the Federal Communications Commission held a workshop to address smartphone thefts and ways to prevent them.[29] Topics discussed included the mobile device theft database and communication of reported smartphone thefts among international, federal, state, and local law enforcement.[30] In that discussion, a representative for the Cellular Telecommunications Industry Association (CTIA) outlined how the database would help phone providers and police compile theft information and track offenders.[31]

However, industry representatives had already responded to the issue by voluntarily agreeing among themselves to provide a kill switch-like solution in smartphones sold after July 2015,[32] and several similar third-party developers's applications were already on the market.[33] Applications such as Find My iPhone, Activation Lock, and Android Device Manager provide varying degrees of protection for lost or stolen phones.[34]

---

25. *Compare FAQ on Lost/Stolen Devices*, *supra* note 17 (stating that time is needed for the database to become known among thieves before it becomes effective), *with* Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2 (arguing that a similar database was ineffective in the United Kingdom and that U.S. phone thefts continue to rise despite use of the database).

26. *See, e.g.*, Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2 (expressing appreciation for the CTIA database but calling for implementation of a kill switch in all smartphones as the next step toward preventing smartphone thefts).

27. *Secure Our Smartphones Initiative Members*, N.Y. ATTORNEY GEN., http://www.ag.ny.gov/sos/initiative-members (last visited June 19, 2014) (on file with the *McGeorge Law Review*); Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2.

28. Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2.

29. Press Release, Fed. Commc'n Comm'n, FCC Announces Workshop to Focus on Prevention of Mobile Device Theft (May 20, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0520/DA-14-685A1.pdf (on file with the *McGeorge Law Review*).

30. *Id.*

31. CTIA, GLOBAL IMEI DATABASE 6 (June 19, 2014), *available at* http://transition.fcc.gov/cgb/events/CTIAJune19th-2014FCC-2.pdf (on file with the *McGeorge Law Review*).

32. *Id.* at 15.

33. Kent German, *Essential Steps for Securing Your Phone, and What Else Can Be Done to Foil Thieves*, CNET (Dec. 11, 2013, 5:04 PM), http://www.cnet.com/how-to/essential-steps-for-securing-your-phone-and-what-else-can-be-done-to-foil-thieves/ (on file with the *McGeorge Law Review*).

34. *Id.*

Despite the solutions available on the market, federal and state legislators have moved forward in their efforts to enact new laws, which purport to give consumers greater security than the available options.[35]

B. Federal Legislators Consider a Kill Switch Bill

Shortly after California State Senator Mark Leno introduced Chapter 275,[36] four U.S. Senators introduced legislation that, if passed, would require cellular phone providers to allow users to render stolen or lost devices inoperable.[37] Congressman José Serrano also introduced a similar bill in the House of Representatives.[38] The Senate and House bills are indistinguishable in language,[39] yet differ in several respects from California's legislation.[40]

Unlike Chapter 275, the federal bills exempt cellular phone companies from the kill switch requirement if they have a similar solution already in place.[41] The federal legislation also allows a manufacturer additional time to comply with the law if needed.[42] The federal law does not specify how the manufacturer must provide the security feature to consumers; it only states that manufacturers must make the security feature available.[43] The federal law provides for a penalty against manufacturers who fail to comply, but leaves the penalty amount up to the Federal Communications Commission.[44]

Federal legislators have also introduced the Mobile Theft Deterrence Act (the MTD Act).[45] The MTD Act punishes a thief who tampers with the identification number[46] of a smartphone or whose theft or hacking[47] of a smartphone involves

---

35. *See* SB 962, 2013–14 Leg., 2013–2014 Sess. (Cal. 2014) (enacted) (requiring smartphones sold after July 1, 2015 to come equipped with theft-deterrent software); S. 2032, 113th Cong. (2014) (introduced Feb. 14, 2014) (requiring software on mobile devices capable of removing user data from a lost or stolen device, preventing that device from being used on a network, preventing reactivation of the device, and allowing restoration of user data if the device is recovered); H.R. 4065, 113th Cong. (2014) (introduced Feb. 14, 2014) (mimicking the requirements of S. 2032).

36. SB 962, 2013–14 Leg., 2013–2014 Sess. (Cal. 2014) (enacted). SB 962 was introduced February 6, 2014. *Complete Bill History of SB 962*, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml;jsessionid=d7c476f8cc8d8cfc800fc5ca345b (last visited Oct. 26, 2014) (on file with the *McGeorge Law Review*).

37. S. 2032, 113th Cong. (2014) (introduced Feb. 14, 2014).

38. H.R. 4065, 113th Cong. (2014) (introduced Feb. 14, 2014).

39. *Compare* S. 2032, 113th Cong. (2014), *with* H.R. 4065, 113th Cong. (2014).

40. *Compare* S. 2032, 113th Cong. (2014), *and* H.R. 4065, 113th Cong. (2014), *with* S.B. 962, 2013–14 Leg., 2013–2014 Sess. (Cal. 2014).

41. S. 2032, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(b)(3)(A)); H.R. 4065, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(b)(3)(A)).

42. H.R. 4065, 133th Cong. § 3(b)(2) (2014) (providing an exemption if an individual can show they require additional time to meet the law's mandates).

43. S. 2032, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(b)(2)); H.R. 4065, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(b)(2)).

44. S. 2032, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(d)); H.R. 4065, 113th Cong. § 3(a) (2014) (enacting 47 U.S.C. § 343(d)).

45. S. 1070, 113th Cong. (2014) (introduced May 23, 2013).

46. An identification number "identifies a specific mobile wireless communications device." *Id.*

tampering with the identification number.[48] Those found guilty of violating the act could serve up to five years in prison.[49]

C. Existing State Law Governing the Interruption of Phone Service

California Public Utilities Code section 7908 allows a government agency to interrupt cellular phone service for public safety reasons.[50] To use the law, a public entity[51] must receive judicial approval.[52] A judge may grant approval if a public entity shows probable cause that the service disruption is necessary to prevent further illegal activity and protect the public from serious and immediate danger.[53] In order to avoid infringing on free speech, the government may suspend service only to the extent reasonably necessary.[54]

Section 7908 was enacted after officials for the Bay Area Rapid Transit System (BART) cut cellular phone service to four stations to stop protestors from coordinating their locations in 2011.[55] BART adopted a policy following the protests that stated the agency could cut cellular phone service if the agency "determine[d] that there [was] strong evidence of imminent unlawful activity that threaten[ed] the safety of [BART] passengers, employees and other members of the public, the destruction of [BART] property, or the substantial disruption of public transit services."[56] The policy did not require BART officials to obtain a court order first.[57]

In enacting Public Utilities Code section 7908, the Legislature found that free speech was threatened when government agencies could stop cellular phone service.[58] The Legislature cited a California Supreme Court case requiring an agency to show probable cause for disrupting communication devices.[59] It also

---

47. Federal law defines hacking as accessing a protected computer without permission and with the intent to defraud. 18 U.S.C. § 1030(a)(4) (2012).

48. S. 1070, 113th Cong. § 2 (2013) (enacting 18 U.S.C. § 515(b)).

49. S. 1070, 113th Cong. § 2 (2013) (enacting 18 U.S.C. § 515(c)).

50. CAL. PUB. UTIL. CODE § 7908(b)(1) (West Supp. 2014).

51. A public entity, for the purposes of the applicable law, is defined as "every local government, including a city, county, city and county, a transit, joint powers, special, or other district, the state, and every agency, department, commission, board, bureau, or other political subdivision of the state, or any authorized agent thereof." *Id.* § 7908(a)(2).

52. *Id.*

53. *Id.* § 7908(b)(1)(A)–(B).

54. *Id.* § 7908(b)(3).

55. *See, e.g.*, Enrique Armijo, *Kill Switches, Forum Doctrine, and the First Amendment's Digital Future*, 32 CARDOZO ARTS & ENT. L.J. 411, 422 (2014) (comparing the BART service interruption to government use of kill switches to prevent protests in Syria, Egypt, Libya, India, and Pakistan).

56. S.F. BAY AREA RAPID TRANSIT DIST., CELL SERVICE INTERRUPTION POLICY 1 (Dec. 1, 2011), *available at* http://www.bart.gov/sites/default/files/docs/final_CSIP.pdf.

57. *Id.*

58. 2013 Cal. Stat. ch. 371, § 1(d)–(f).

59. *Id.* § 1(g) (citing Sokol v. Public Utils. Comm'n, 65 Cal. 2d 247, 256, 418 P.2d 265, 271 (1966). *Sokol* held that a police agency must receive approval from an impartial tribunal before terminating a

interpreted the first amendment of the U.S. Constitution and article one, section two of the California Constitution as providing free speech protection to mobile devices and communication.[60]

III. CHAPTER 275

Chapter 275 requires smartphones sold in the state after July 1, 2015, to give users the ability to make the "essential features"[61] of a stolen or missing smartphone inoperative.[62] Upon retrieving a lost or stolen smartphone, the owner must be able to restore the essential features.[63] Additionally, to deter thieves, a smartphone manufacturer that incorporates this security requirement into the device must ensure that it can withstand a "hard reset."[64] After July 1, 2015, a smartphone sold in California must, as its default setting, prompt the buyer during the initial set up of the phone to enable the protection required by Chapter 275 if it is not already a part of the phone's default settings.[65] Also, Chapter 275 allows smartphone providers to offer security features in addition to the required protective software.[66]

Chapter 275 imposes civil penalties between $500 and $2,500 if a company knowingly sells a smartphone without the required features.[67] However, there are no civil penalties if the security solution fails due to the acts of a third party of which the retailer is unaware.[68] A private individual does not have a cause of action against a retailer for selling a smartphone that cannot be rendered inoperable.[69] Additionally, if the government wants to "interrupt" the use of a

consumer's telephone service. *Sokol*, 65 Cal. 2d at 256, 418 P.2d at 271; *see also* Goldin v. Public Util. Comm'n, 23 Cal. 3d 638, 666–67, 592 P.2d 289, 307–08 (1979) (upholding commission's rule and process for interrupting telephone service as in compliance with state and federal law).

60. 2013 Cal. Stat. ch. 371, § 1(d).

61. The "'[e]ssential features' of a smartphone" include voice communications, Internet browsing, and access to applications. CAL. BUS. & PROF. CODE § 22761(a)(2) (enacted by Chapter 275).

62. *Id*. § 22761(b)(1) (enacted by Chapter 275). This does not include the ability to call 911 or receive emergency alerts. *Id*. § 22761(g) (enacted by Chapter 275).

63. *Id.*

64. *Id.*; *see also id.* § 22761(a)(3) (enacted by Chapter 275) (defining a "hard reset" as the ability to return the phone to its factory settings).

65. *Id*. § 22761(b)(1) (enacted by Chapter 275). A smartphone purchaser can choose to disable the security feature that comports with Chapter 275 as long as the owner, or an individual designated by the phone's owner, is the one who disables the security requirement. *Id.* § 22761(b)(2) (enacted by Chapter 275); s*ee also* SENATE RULES COMMITTEE, UNFINISHED BUSINESS, at 2 (Aug. 4, 2014) (requiring a prompt during set-up of smartphone).

66. BUS. & PROF. § 22761(f) (enacted by Chapter 275).

67. *Id.* § 22761(c) (enacted by Chapter 275).

68. *Id.* § 22761(c)–(d) (enacted by Chapter 275).

69. *Id.* § 22761(c) (enacted by Chapter 275). Only the Attorney General or a district or city attorney can enforce Chapter 275. *Id.*

smartphone with Chapter 275's solution, it must do so in accordance with existing law.[70]

IV. ANALYSIS

This section examines whether Chapter 275's proposed solution will deter smartphone thefts, weighs concerns over whether a kill switch grants the government control of smartphones, and explores whether consumers need Chapter 275's security requirement given that smartphone anti-theft technology is already available.

A. Will Chapter 275 Deter Smartphone Thefts?

Smartphone theft statistics present conflicting evidence as to whether a kill switch is the most effective means of providing consumer protection.[71] The CTIA, which advocates for the smartphone theft database launched in 2013, argues that more time is needed to determine the success of the program because it relies on consumers reporting thefts and efforts are ongoing to expand the database into foreign countries.[72] Opponents of the database point to the failure of a similar one started in the United Kingdom that did not deter smartphone thefts.[73]

Additionally, there are other potential alternatives to requiring a kill switch.[74] In 2014, San Francisco transportation officials reported 77% less smartphone thefts due to an increase in police officer patrols in and around public transportation areas.[75] However, the extra patrols were supported by a $1 million federal grant, which may not be available long term.[76] San Francisco law enforcement officers are trying to catch smartphone thieves by targeting buyers and sellers of the stolen devices.[77] The officers dress in plain clothes, target high

---

70. *Id.* §22761(e) (enacted by Chapter 275). State officials who seek to interrupt the service of a smartphone must follow California Public Utilities Code section 7908. *Id. See* Part II.C for further discussion of California Public Utilities Code section 7908.

71. ASSEMBLY COMMITTEE ON UTILITIES & COMMERCE, COMMITTEE ANALYSIS OF SB 962, at 2–3 (June 23, 2014).

72. *FAQ on Lost/Stolen Devices*, *supra* note 17.

73. *See, e.g.*, Press Release, N.Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2 (arguing that a similar database was ineffective in the United Kingdom).

74. *See* ASSEMBLY COMMITTEE ON UTILITIES & COMMERCE, COMMITTEE ANALYSIS OF SB 962, at 2 (June 23, 2014) (describing alternate approaches including increased law enforcement patrols and stolen device databases).

75. *Id.*; Press Release, S.F. Mun. Transp. Agency, Crime on Muni Reduced by 30 Percent (May 12, 2014), *available at* http://www.sfmta.com/es/news/press-releases/crime-muni-reduced-30-percent (on file with the *McGeorge Law Review*).

76. ASSEMBLY COMMITTEE ON UTILITIES & COMMERCE, COMMITTEE ANALYSIS OF SB 962, at 2 (June 23, 2014).

77. Gerry Smith, *Undercover Police Stings Target Front Lines of Stolen iPhone Market*, HUFFINGTON POST (June 28, 2013, 4:13 PM), http://www.huffingtonpost.com/2013/04/26/police-sting-stolen-iphones_n_313

profile districts where stolen phones are sold, and then arrest sellers once a transaction is complete.[78] However, this use of undercover officers is controversial in that it may amount to unlawful entrapment.[79]

Moreover, opponents of Chapter 275 say it has the potential to harm competition through over-regulation.[80] As an alternative, the CTIA argues that the growth of the smartphone theft database is a better solution.[81] Smartphone manufacturers also advocate for the growth of the smartphone theft database and for the passage of the MTD Act,[82] which penalizes tampering with a smartphone's identification number more harshly than current California law.[83] Smartphone manufacturers support the MTD Act over Chapter 275 because they view it as one element of a comprehensive answer to smartphone thefts that does not stifle growth, as they claim the kill switch does, stops reactivation of a stolen phone, and deters thefts.[84]

However, kill switch advocates note that thefts fell by 17% in New York City and 38% in San Francisco after Apple introduced a kill switch option to its users.[85] Proponents of the kill switch argue that it is more effective than a database because the database's success depends on consumers reporting lost or stolen cellular phones and because the database does not reach many foreign countries where stolen phones are shipped.[86] Further, even with a kill switch, a smartphone may remain attractive to thieves who would sell it for parts.[87]

8609.html (on file with the *McGeorge Law Review*).

78. *Id.*

79. *Id.*

80. *See* SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF SB 962, at 6 (May 6, 2014) (indicating that over regulation may serve as a market barrier to new technology or may lead to the development "of an anticompetitive and anti-consumer choice environment").

81. *See U.S. Wireless Industry Announces Steps to Help Deter Smartphone Thefts and Protect Consumer Data,* CTIA (Apr. 10, 2014), http://www.ctia.org/resource-library/press-releases/archive/deter-smartphone-thefts-and-protect-consumer-data (on file with the *McGeorge Law Review*) (outlining the steps the CTIA developed to deter smartphone thefts).

82. *How to Deter Smartphone Thefts and Protect Your Data*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data (last visited Oct. 28, 2014) (on file with the *McGeorge Law Review*).

83. *Compare* S. 1070, 113th Cong. § 2 (2013) (enacting 18 U.S.C. § 515(b)–(c)) (making tampering with the IMEI number of a smartphone a federal crime punishable by up to five years in prison), *with* CAL. PENAL CODE § 490 (West 2010) (requiring a person convicted of petty theft to pay a fine of up to $1,000 and/or spend up to six months in county jail).

84. Damon Poeter, *Schumer Introduces Bill to Make Cell Phone ID Tampering a Crime*, PCMAG (May 24, 2013, 2:03 PM), http://www.pcmag.com/article2/0,2817,2419491,00.asp (on file with the *McGeorge Law Review*); *FAQ on Lost/Stolen Devices*, *supra* note 17.

85. ASSEMBLY COMMITTEE ON UTILITIES & COMMERCE, COMMITTEE ANALYSIS OF SB 962, at 2 (June 23, 2014).

86. *Id.* at 8.

87. *Id*. at 3.

As a result, the solution required by Chapter 275 may not be as strong a deterrent to thefts because similar programs are already in place and inoperable phones may still have value to thieves.[88]

B. The Kill Switch May Allow the Government to Interrupt Phone Service

Some technology industry leaders who oppose mandating a kill switch in every smartphone believe that Chapter 275's solution provides government officials a "backdoor" into every mobile device.[89] This concern is due to vague language in Chapter 275 defining who qualifies as an "authorized user" allowed to activate a kill switch,[90] which is not defined in Chapter 275.[91] Also, Chapter 275's inclusion of Public Utilities Code section 7908 lays out the steps for a public entity to interrupt cellular phone service.[92] As one opponent group points out, as a result of Chapter 275, "a large barrier [to government interruption of cellular phone service]—technical access to our phones—will have disappeared."[93] However, the concern over the government intruding into smartphones may be unfounded.[94] The potentially invasive aspect of the kill switch is its ability to use geolocation software, which users have to approve.[95] Chapter 275 addressed this concern by requiring that users have the power to disable the kill switch if they want.[96]

Proponents of section 7908 believed it would protect the right to free speech while providing a way for law enforcement to act in the interests of public safety.[97] In supporting section 7908, proponents, including AT&T and TechNet (which had concerns about the kill switch bill), essentially described the law as a compromise between not violating private rights and allowing law enforcement to react when necessary.[98] Further, supporters said the section acknowledged that providers need control over their systems.[99]

---

88. *See id.* at 2–3 (stating there is evidence anti-theft features on phones decrease thefts, but inoperable phones may still be sold for their parts).

89. Letter from Hannah Fakhoury, Staff Attorney, Adi Kamdar, Activist & Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation, to Assemblymember Susan Bonilla, Chair, Assembly Business, Professions & Consumer Protection Committee (June 16, 2014) (on file with the *McGeorge Law Review*).

90. *Id.*

91. CAL. BUS. & PROF. CODE § 22761(a) (enacted by Chapter 275).

92. *Id.*

93. Press Release, N,Y. Attorney Gen. Eric T. Schneiderman, *supra* note 2; S.F. POLICE DEP'T, *supra* note 6, at 47.

94. SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS, COMMITTEE ANALYSIS OF SB 962, at 5–6 (Mar. 24, 2014).

95. *See id.*

96. BUS. & PROF. § 22761(b)(1) (enacted by Chapter 275).

97. SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF SB 380, at 6 (Sept. 5, 2013).

98. *Id.*

99. *Id.*

However, opponents of Chapter 275 state that it goes too far by giving the government the potential for control through section 7908[100] and hindering innovation in the smartphone industry.[101] Critics of the chapter, including the CTIA, state that a kill switch mandates a "'one-size-fits-all' approach" as it limits technological advancement and makes it easier for thieves to overcome the legally mandated requirement because there will be only one security measure to disable.[102] Further, the CTIA argues that the requirements of the kill switch can become outdated as technology advances and that the legislature will be unable to keep up with new innovations used to overcome the the kill switch.[103] But this concern is potentially mitigated by the fact that Chapter 275 allows manufacturers to add additional security measures, thus enabling them to advance with technology.[104]

C. Is Chapter 275 Already Obsolete?

The kill switch requirement and the battle to prevent it may seem unnecessary considering that many smartphone providers already offer consumers the ability to remotely disable their lost or stolen devices.[105] In addition, in 2014, several smartphone manufacturers signed a voluntary commitment to offer anti-theft programs to consumers.[106] Thus, Chapter 275's mandate will not require anything different than what many manufacturers will already offer in 2015.[107]

Cellular phone manufacturers argue that requiring a kill switch makes consumers more vulnerable to hackers because it would impose just one security measure to override.[108] Because technology becomes outdated quickly, it is difficult for the law to keep up.[109] Supporters counter that the need to deter thieves is important enough to require a standard solution.[110] Further, the law

---

100. Letter from Hannah Fakhoury, Adi Kamdar, & Lee Tien to Susan Bonilla, *supra* note 89.

101. SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF SB 962, at 6 (May 6, 2014).

102. *FAQ on Lost/Stolen Devices*, *supra* note 17.

103. *Id.*

104. CAL. BUS. & PROF CODE § 22761(f) (enacted by Chapter 275).

105. ASSEMBLY COMMITTEE ON UTILITIES & COMMERCE, COMMITTEE ANALYSIS OF SB 962, at 2–3 (June 23, 2014) (indicating Apple already offers a kill switch application, while Microsoft and Google will include theft deterrent programs in the next editions of their smartphones).

106. *FAQ on Lost/Stolen Devices*, *supra* note 17. Companies that signed the commitment include: "Apple Inc.; Asurion; AT&T; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics MobileComm USA, Inc.; Motorola Mobility LLC; Microsoft Corporation; Nokia, Inc.; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon Wireless; and ZTE USA, Inc." *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. ASSEMBLY COMMITTEE ON BUSINESS, PROFESSIONS AND CONSUMER PROTECTION, COMMITTEE ANALYSIS OF SB 962, at 4 (Aug. 4, 2014).

relieves providers of any liability if a hacker disables the solution as long as the company is unaware prior to the sale that an aspect of the software was vulnerable.[111] However, as technology evolves and solutions do become vulnerable to attack, it appears there will be an ongoing need for manufacturers to develop new ways of deterring thefts.[112]

Given that market forces are already driving smartphone manufacturers to give consumers the security solutions they desire, Chapter 275 does not have a significant impact other than requiring a prompt for the user to choose to download the security function.[113]

V. CONCLUSION

Chapter 275 aims to protect smartphone consumers from a growing number of thieves by requiring manufacturers to install a kill switch function in their devices that gives owners, or arguably whoever qualifies as an authorized user, the ability to render the core functions of their phones inoperative when phones are lost or stolen.[114] However, many smartphones on the market already offer this function or something similar,[115] and manufacturers have already agreed to provide a security function in all devices sold after July 2015.[116] Thus, aside from whether the law will stifle technological growth[117] or limit free speech,[118] the most important question is whether the law is necessary at all.[119] As consumers can choose among the various features available in smartphones, they have the option to consider various security features prior to purchasing a device.[120] With the passage of Chapter 275, smartphone owners receive some protection from thieves but it is not the only solution needed to stop smartphone thefts.[121] A more

---

111. *Id.* at 5.

112. *See id.* (stating liability protection is only applicable at the time of sale and does not cover subsequent harms).

113. *Compare FAQ on Lost/Stolen Devices*, *supra* note 17 (announcing that smartphones will give users a security function already on the phone or available for download that remotely deletes data, allows the phone to be made inoperable, allows only an authorized user to reactive the phone, and allows the owner to restore the phone to its original function), *with* CAL. BUS. & PROF. CODE § 22761(b)(1) (enacted by Chapter 275) (mandating that a smartphone prompt its owner to enable anti-theft software that allows the owner to make the phone inoperable, reactivate the phone, and restore the phone's features).

114. SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS, COMMITTEE ANALYSIS OF SB 962, at 1 (Mar. 24, 2014).

115. German, *supra* note 33.

116. *FAQ on Lost/Stolen Devices*, *supra* note 17.

117. SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF SB 962, at 6 (May 6, 2014) ("[I]t is also conceivable that a government entity may attempt to use kill switch technology to intentionally cut off service of protestors or government critics, which is not uncommon in countries that lack free speech protection.").

118. Letter from Hannah Fakhoury, Adi Kamdar, & Lee Tien to Susan Bonilla, *supra* note 89.

119. *See FAQ on Lost/Stolen Devices*, *supra* note 17 (indicating that smartphone manufacturers have already volunteered to make anti-theft software available on their devices by 2015).

120. German, *supra* note 33.

121. *Id.*

comprehensive approach to theft deterrence, such as increased reporting requirements of stolen phones from law enforcement and manufacturers, may be the next step in targeting thieves instead of requiring manufacturers to include additional security features.[122]

122. *See* discussion *supra* notes 17–25 and accompanying text (discussing the stolen phone database).