SENATE RULES COMMITTEE SB 962
Office of Senate Floor Analyses
1020 N Street, Suite 524
(916) 651-1520 Fax: (916) 327-4478

UNFINISHED BUSINESS

Bill No: SB 962
Author: Leno (D), et al.
Amended: 8/4/14
Vote: 21

SENATE ENERGY, UTIL. & COMMUNIC. COMM.: 6-2, 4/1/14
AYES: Padilla, Corbett, DeSaulnier, Hill, Pavley, Wolk
NOES: Fuller, Knight
NO VOTE RECORDED: Block, Cannella, De León

SENATE FLOOR: 26-8, 5/8/14
AYES: Beall, Block, Cannella, Corbett, Correa, De León, DeSaulnier, Evans, Gaines, Galgiani, Hancock, Hernandez, Hill, Hueso, Jackson, Lara, Leno, Lieu, Liu, Mitchell, Monning, Padilla, Pavley, Roth, Steinberg, Wolk
NOES: Anderson, Berryhill, Fuller, Huff, Morrell, Vidak, Walters, Wyland
NO VOTE RECORDED: Calderon, Knight, Nielsen, Torres, Wright, Yee

ASSEMBLY FLOOR: 53-20, 8/7/14 - See last page for vote

SUBJECT: Advanced mobile communications devices

SOURCE: San Francisco, District Attorney George Gascón

DIGEST: This bill requires smartphones manufactured after July 1, 2015, and sold in California to contain a technological solution at the time of sale that will render the essential features of the smartphone inoperable when not in the possession of the authorized user, and also provides a civil penalty for violations and limits retail liability if the solution is circumvented.

Assembly Amendments refine the definitions of "smartphone," "essential features," and "hard reset;" clarify that any smartphone model that was first

CONTINUED

introduced prior to January 1, 2015, that cannot reasonably be reengineered to support the manufacturer's or operating system provider's technological solution, is not subject to the requirements of this bill; add specific protections for retailers, manufacturers and operating system providers; and state that no local government shall adopt their own ordinances related to technological solutions for smartphones.

ANALYSIS:

Existing law:

1. Provides that theft - the stealing, taking, or driving away with the personal property of another - is a misdemeanor when the value of the property does not exceed $950 and is punishable by fines and up to one year in the county jail.

2. Requires all providers of wireless and Internet-based communications services to enable customers to call 911 for emergency services, and establishes dates for enabling text to 911 and Next Generation 911.

This bill:

1. Requires any smartphone manufactured on or after July 1, 2015, and sold in California after that date to include a technological solution at the time of sale, to be provided by the manufacturer or operating system provider, that once initiated and successfully communicated to the smartphone, can render the essential features, as defined, of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user.

2. Requires the smartphone, during the initial device setup process, to prompt an authorized user to enable the technological solution.

3. Requires the technological solution to be reversible, so that if an authorized user obtains possession of the smartphone after the essential features of the smartphone have been rendered inoperable, the operation of those essential features can be restored by an authorized user.

4. Provides that the technological solution may consist of software, hardware, or a combination of both software and hardware.

5. Requires that the technological solution be able to withstand a hard reset or operating system downgrade.

CONTINUED

6. Requires that the technological solution prevent reactivation of the smartphone on a wireless network except by an authorized user.

7. Requires that an authorized user of a smartphone be able to affirmatively elect to disable or opt-out of enabling the technological solution at any time.

8. Requires that the physical acts necessary to disable or opt-out of enabling the technological solution may only be performed by the authorized user or a person specifically selected by the authorized user to disable or opt-out of enabling the technological solution.

9. Exempts from the anti-theft technological solution requirements of these provisions any smartphone model that was first introduced prior to January 1, 2015, which cannot reasonably be reengineered to support the manufacturer's or operating system provider's technological solution, including if the hardware or software cannot support a retroactive update.

10. Provides that the knowing retail sale of a smartphone in California in violation of these requirements may be subject to a civil penalty of not less than $500, not more than $2,500, per smartphone sold in California in violation of these provisions.

11. Requires any suit to impose a civil penalty to be brought by the Attorney General, a district attorney, or a city attorney.

12. Provides that a failure of the technological solution due to hacking or other third-party circumvention may be considered a violation for purposes of the civil penalty if, at the time of sale, the seller had received notification from the manufacturer or operating system provider that the vulnerability cannot be remedied by a software patch or other solution.

13. Specifies that there is no private right of action to enforce these provisions.

14. Provides that the retail sale in California of a smartphone shall not result in any private civil liability to the seller from that retail sale alone if the liability results from or is caused by failure of a technological solution, including any hacking or other third-party circumvention, unless at the time of sale the seller had received notification from the manufacturer or operating system provider that the vulnerability cannot be remedied by a software patch or other solution.

CONTINUED

15. Provides that nothing in these provisions preclude a suit for civil damages on any other basis outside of the retail sale transaction, including, but not limited to, a claim of false advertising.

16. States that nothing in these provisions prohibit a network operator, device manufacturer, or operating system provider from offering a technological solution or other service in addition to the technological solution required to be provided by the device manufacturer or operating system provider.

17. States that nothing in these provisions require a technological solution that is incompatible with, or renders it impossible to comply with, obligations under state and federal law and regulation related to any of the following:

    A. The provision of emergency services through the 911 system, including text to 911, bounce-back messages, and location accuracy requirements;

    B. Participation in the wireless emergency alert system; and

    C. Participation in state and local emergency alert and public safety warning systems.

18. Defines the term "smartphone" to mean a cellular radio telephone or other mobile voice communications handset device (but not a radio cellular telephone commonly referred to as a "feature" or "messaging" telephone, laptop, a tablet device, or a device that only has electronic reading capability), that includes all of the following features:

    A. Utilizes a mobile operating system;

    B. Possesses the capability to utilize mobile software applications, access and browse the Internet, utilize text messaging, utilize digital voice service, and send and receive email;

    C. Has wireless network connectivity; and

    D. Is capable of operating on a long-term evolution network or successor wireless data network communication standards.

19. Defines the "essential features" of a smartphone to be the ability to use the smartphone for voice communications, text messaging, and the ability to browse the Internet, including the ability to access and use mobile software

CONTINUED

applications. Essential features do not include any functionality needed for the operation of the technological solution, nor does it include the ability of the smartphone to access emergency services by a voice call or text to the numerals '911,' the ability of a smartphone to receive wireless emergency alerts and warnings, or the ability to call an emergency number pre-designated by the owner.

20. Defines the term "hard reset" to mean the restoration of a smartphone to the state it was in when it left the factory through processes commonly termed a factory reset or master reset.

21. Defines the term "Sold in California," or any variation thereof, to mean that the smartphone is sold at retail from a location within the state, or the smartphone is sold and shipped to an end-use consumer at an address within the state. Sold in California does not include a smartphone that is resold in the state on the secondhand market or that is consigned and held as collateral on a loan.

22. Makes findings and declarations such the enactment of a uniform policy to deter the theft of smartphones and to protect the privacy of owners of stolen smartphones is a matter of statewide concern and that no city, county, or city and county shall impose requirements on manufacturers, operating system providers, wireless carriers, or retailers relating to technological solutions for smartphones.

23. Makes findings and declarations related to the prevalence and ramifications of smartphone theft in the United States.

Background

As smartphones continue to transform all aspects of modern life, they also have caused a crime epidemic. More than 90% of all Americans own a mobile device, and nearly 60% a smartphone. The high resale value of smartphones and other hand-held mobile devices like tablets, and their relatively small size, make them prime targets for thieves. Many published reports document a dramatic increase of smartphone theft. According to reports summarized by the San Francisco District Attorney's Office:

- Most robberies now involve the theft of a smartphone;

- In 2012, more than 50% of all robberies in San Francisco and 75% in Oakland involved the theft of a mobile device; and

CONTINUED

- An estimated 1.6 million Americans were victimized for their smartphones in 2012.

The Federal Communications Commission, law enforcement, and industry collaborated on efforts to address the problem in 2012. These included providing consumers more security options on devices and automatic prompts to establish passwords and launching a public education campaign urging consumers to use security apps that enable them to remotely locate, lock and wipe devices. A national database was established to help prevent lost or stolen phones from being reactivated. Wireless carriers use the database to check whether a device presented to them has been reported lost or stolen and, if so, it will not allow service to be established. Its effectiveness depends on consumers reporting a lost or stolen phone. Industry reports that efforts are underway to link more foreign carriers and countries to the database. Without that international cooperation, stolen phones resold in foreign countries continue to have value.

Industry continues to introduce new and more sophisticated security solutions for consumers. These include options such as Apple's "Find My iPhone" with "Activation Lock" feature that allows a person who has lost or stolen an iPhone to remotely log into a hosted platform and send a signal to lock the device and make it unusable without the original owner's security passcode established when the device was purchased. Other solutions include Samsung's "Reactivation Lock" and Android's "Lo Jack." Some solutions are built into the device or downloaded as an app, some with a fee.

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

SUPPORT: (Verified 8/7/14)

San Francisco, District Attorney George Gascón (source)
Alameda County District Attorney's Office
Associated Students of the University of California
Association of Chief Police Officers of the United Kingdom
Association of Orange County Deputy Sheriffs Association
Berkeley City Council
California College & University Police Chiefs Association
California District Attorneys Association
California Fraternal Order of Police
California Pawnbrokers Association
California Police Chiefs Association

CONTINUED

California State Sheriffs' Association
California Transit Association
Cities of Emeryville, Los Angeles, Oakland, San Diego, San Francisco, Santa Ana and Thousand Oaks
City and County of San Francisco
City of Los Angeles, Mayor Eric Garcetti
City of Los Angeles, Police Chief Charlie Beck
City of Oakland, City Council Pro Tem Rebecca D. Kaplan
Consumer Action
Consumer Federation of California
Consumers Union
Crime Victims United of California
Hayward Police Department
Long Beach Police Officers Association
Los Angeles County Deputy Sheriffs Association
Los Angeles County District Attorney's Office
Los Angeles Police Protective League
Los Angeles Professional Peace Officers Association
Los Angeles, City Attorney Michael N. Feuer
Mayors and Councilmembers Association of Sonoma County
Metropolitan Police Service of London, U.K.
Neighborhood Crime Prevention Councils of Oakland
Oakland Chamber of Commerce
Oakland City Council
Oakland Police Department, Chief of Police Sean C. Whent
Oakland, Mayor Jean Quan
Riverside Sheriffs Association
Sacramento County Deputy Sheriffs Association
San Diego, District Attorney Bonnie Dumanis
San Francisco Bay Area Transit District
San Francisco Bay Area Transit District Police Department
San Francisco Municipal Transportation Agency
San Mateo County Police Chiefs Association
San Mateo County Sheriffs Association
San Mateo, District Attorney Steve Wagstaffe
Santa Ana Police Officers Association
Santa Clara, District Attorney Jeff Rosen
Secure Our Smartphones (S.O.S.) Initiative
Temescal Merchants Association
The Utility Reform Network

CONTINUED

OPPOSITION: (Verified 8/7/14)

CalChamber
CTIA, the Wireless Association
Electronic Frontier Foundation
League of California Cities
Los Angeles Area Chamber of Commerce
San Jose Silicon Valley Chamber of Commerce
Silicon Valley Leadership Group
TechAmerica
TechNet

ARGUMENTS IN SUPPORT: According to the author "California is experiencing an epidemic of smartphone thefts, many of which turn violent.… There are existing, very serious penalties for theft and robbery in California. However, the epidemic nature of this particular crime is so widespread that enforcement agencies are overwhelmed. That is why removing the value of a stolen device on the black market is the most effective way to deter would be criminals, and this bill will do just that by requiring that smartphones sold in California come pre-equipped with theft deterrent technology.…"

ARGUMENTS IN OPPOSITION: The San Jose Silicon Valley Chamber of Commerce "believes, as one of its guiding principles, that private sector solutions should be sought whenever possible to address public concerns. While we applaud the goal to decrease theft and increase privacy, we feel that SB 962, though well-intentioned, would not achieve that ultimate outcome. Most operating systems developed in Silicon Valley already possess the capability to remotely lock, erase, or disable their mobile devices (including Apple's IOS and Microsoft's Windows Phone). Also, as of late last year, all four major national wireless carriers had begun participation in the international database of lost or stolen4GLTE phones."

ASSEMBLY FLOOR: 53-20, 8/7/14
AYES: Achadjian, Alejo, Ammiano, Bloom, Bocanegra, Bonilla, Bonta, Bradford, Brown, Buchanan, Ian Calderon, Campos, Chau, Chesbro, Conway, Cooley, Dickinson, Eggman, Fong, Gatto, Gomez, Gonzalez, Gordon, Gorell, Gray, Roger Hernández, Holden, Jones-Sawyer, Levine, Lowenthal, Maienschein, Medina, Mullin, Muratsuchi, Nazarian, Nestande, Pan, John A. Pérez, V. Manuel Pérez, Quirk, Rendon, Ridley-Thomas, Rodriguez, Salas, Skinner, Stone, Ting, Weber, Wieckowski, Wilk, Williams, Yamada, Atkins

CONTINUED

NOES: Allen, Chávez, Dababneh, Dahle, Daly, Donnelly, Frazier, Beth Gaines, Grove, Hagman, Harkey, Jones, Logue, Melendez, Olsen, Patterson, Perea, Quirk-Silva, Wagner, Waldron
NO VOTE RECORDED: Bigelow, Fox, Garcia, Hall, Linder, Mansoor, Vacancy

JG:e 8/8/14 Senate Floor Analyses

SUPPORT/OPPOSITION: SEE ABOVE

****** END ******