File No. 140449

Committee Item No._____
Board Item No. 32

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee_____ Date_____

Board of Supervisors Meeting Date May 6, 2014

Cmte	Board	
☐	☐	Motion
☐	☒	Resolution
☐	☐	Ordinance
☐	☐	Legislative Digest
☐	☐	Budget Analyst Report
☐	☐	Legislative Analyst Report
☐	☐	Introduction Form (for hearings)
☐	☒	Department/Agency Cover Letter and/or Report
☐	☐	MOU
☐	☐	Grant Information Form
☐	☐	Grant Budget
☐	☐	Subcontract Budget
☐	☐	Contract/Agreement
☐	☐	Award Letter
☐	☐	Application
☐	☐	Public Correspondence

OTHER (Use back side if additional space is needed)

☐ ☐ _____
☐ ☐ _____
☐ ☐ _____

Completed by: Joy Lamug Date May 1, 2014
Completed by:_____ Date_____

An asterisked item represents the cover sheet to a document that exceeds 20 pages. The complete document is in the file.

FILE NO. 140449 RESOLUTION NO.

[Supporting Senate Bill 962 (Leno) - Smartphone Theft Prevention]

Resolution supporting Senate Bill 962, introduced by Senator Leno, the Smartphone Theft Prevention Act, to require the installation of theft-deterring technological solutions on all smartphones sold in the State of California.

WHEREAS, The theft of mobile devices accounts for one third of all property crimes in the United States, making it the number one property crime; and,

WHEREAS, Smartphone theft accounts for over half of all robberies in the City and County of San Francisco; and,

WHERAS, Smartphone users are easy targets because of how easily devices can be stolen and re-sold; and,

WHEREAS, Mobile device manufacturers and service providers have a corporate responsibility to ensure the users of their services and products are not targeted or victimized; and,

WHEREAS, Street-level crime supplies a vast global black market in stolen personal devices; and,

WHEREAS, There is a need for a ubiquitous theft prevention solution such as a "kill switch" that would act as a strong disincentive to curtail the behavior of thieves; and,

WHEREAS, The existing Federal Communication Commission stolen smartphone database has not proven effective due to placing the burden on the victim to add it to the database, its limitation to the big four domestic carriers, and its inapplicability to phones stolen and then sold abroad; and,

WHEREAS, The wireless industry earns an estimated $30 billion annually from the replacement of lost or stolen devices and $7.8 billion in insurance protection plan premiums; and,

WHEREAS, The wireless industry has previously rejected the voluntarily installation of "kill switch" technology; and,

WHEREAS, SB 962, the Smartphone Theft Prevention Act, would require all advanced communications devices (smartphones and tablets) sold in California to come pre-equipped with a theft-deterring technological solution that renders the essential functions of the device useless when stolen; and,

WHEREAS, SB 962 would allow the consumer to affirmatively opt-out of using the technological solution, but every device must come pre-equipped and enabled with this technology in order for the deterrent value of the solution to be as effective as possible; and,

WHEREAS, SB 962 would not require any solution that infringes on the individual's privacy; and

WHEREAS, The effect of SB 962 would be to remove the re-sale value of stolen devices, thus reducing the current incentive for thieves to prey on smartphone users; and

WHEREAS, San Francisco District Attorney George Gascon co-chairs the global effort Secure Our Smartphones and has worked tirelessly to support SB 962 and prevent smartphone theft through the installation of kill switch technology; and

WHEREAS, The California State Senate failed to vote in support of SB 962 on April 24, 2014, but could take the measure up again in May 2014; now, therefore be it

RESOLVED, That the Board of Supervisors of the City and County of San Francisco urges the California State Legislature to pass SB 962, the Smartphone Theft Prevention Act.

Smartphone Talking Points

Smartphone theft is a global epidemic that urban centers around the world are facing. The experience for millions of victims every year is traumatic and sometimes even violent. Smartphone theft also leaves victims fearful of their private information being exposed and exploited, costs them several hundreds of dollars.

Recently, smartphone manufacturers have agreed to equip phone with an anti-theft deterrence device. However, it falls short of what American wireless consumers need to effectively end the epidemic of smartphone theft.

The trouble with the voluntary agreement is that the solutions will not be enabled by default. The steps to activate anti-theft measures are also often unclear and these protections are ONLY effective if they are on virtually every device. If thieves can't tell which phones have a "kill switch" enabled, and which ones do not, everyone is vulnerable to victimization.

SB 962 makes it so thieves aren't left guessing - there will be no secondhand market for a stolen smartphone because you can't sell a device that doesn't work. By installing and enabling a kill switch on all phones, stolen devices are inoperable on any network, anywhere in the world. With the successful passage of this bill, thieves will get the message that stealing smartphones is a useless proposition, that a stolen smartphone will be as valuable as a paperweight.

As a result, the American wireless consumer can have a little more comfort in knowing that they're not going to be targeted for their smartphone.

California truly has an opportunity to lead the way and end this public safety crisis. Though this bill did not pass the first time, it is imperative that we support it when it is up for a vote again.

Smartphone Talking Points

- Make no mistake; this is a global epidemic that urban centers around the world are facing.

- The experience for millions of victims every year is traumatic, leaving them fearful and out several hundreds of dollars. But for others, the incident can result in serious injury- and in the most tragic incidents, death.

- These street level thieves feed a massive global marketplace for stolen phones too large or lucrative for any single community to stop. In fact, smartphone theft has become so lucrative the Columbian drug cartels are now trafficking in stolen smartphones.

- In Hong Kong, for example, iPhones trafficked from the U.S or elsewhere fetch upward of $2,000 a piece.

- The industry has failed to safeguard their products- and their customers are bearing the brunt of this failure.

- These thieves will not stop until the incentive is removed.

- Recently, smartphone manufacturers have agreed to equip the phones they sell with an anti-theft deterrence device.

- It's great that the industry is finally acknowledging that both the problem and solution is in their hands. This is a welcome step forward, but it falls short of what American wireless consumers need to effectively end the epidemic of smartphone theft.

- The trouble with the voluntary agreement offered by CTIA is that the solutions will not be enabled by default.

- These proposed solutions require smartphone owners to seek out the features and turn it on.

- We cannot rely on consumers to seek out this technology and to take steps that are often unclear in order to protect themselves and every other wireless consumer.

- These solutions are ONLY effective if they are on virtually every device.

- As evidenced by the increase in smartphone theft across the country, existing solutions that put the onus on the consumer to seek out and turn on the technology are not effective.

- This is because thieves can't tell which phones have the feature enabled, and which ones do not, which leaves everyone vulnerable to victimization.

- As currently deployed by the manufacturers, these solutions are not on enough smartphones to deter thieves.

- For the thieves, it's simple math. If a thief can resell 4 of the 5 phones they steal, the incentive to victimize wireless consumers is still intact.

- That is the crux of SB 962- this legislation will shatter this incentive by ensuring these existing solutions are standard on all devices.

- This legislation makes it so thieves aren't left guessing- there will be no secondhand market for a stolen smartphone because you can't sell a device that doesn't work.

- That is what SB 962 proposes to do- with its successful passage, thieves will get the message that stealing smartphones is a useless

proposition, that a stolen smartphone will be as valuable as a paperweight.

- As a result, the American wireless consumer can have a little more comfort in knowing that they're not going to be targeted for their shiny new smartphone.

- To be absolutely clear, the industry has the capacity to implement these solutions now, ubiquitously, but they have chosen not to.

- Whether their inaction, and in some cases- blatant obstruction- is a result of a lack of motivation, or the profits they stand to lose, these corporations have a responsibility to their customers.

- California truly has an opportunity to lead the way and end this pubic safety crisis. The potential to end this global epidemic is very real.

SB 962 (Leno): Smartphone Theft Prevention

FACT VERSUS FICTION
Responses to CTIA's Inaccurate & Misleading Floor Alert

SB 962 addresses the skyrocketing rate of smartphone robberies in California which have reached unprecedented levels and often turn violent due to the high value of the devices on the illegal black market.

SB 962 (Leno) enjoys a lengthy list of support from statewide law enforcement professionals, major city police chiefs, mayors, cities, transit agencies, student groups and consumer protection advocates. The wireless industry issued a "floor alert" about SB 962 on March 24th, which made several claims that called into question the approach of protecting consumers by requiring theft-deterrent technology on smartphones. These industry talking points are debunked below. Please contact Max Szabo with the San Francisco District Attorney's Office at (415) 553-9089 with any questions regarding this bill.

- **Fiction: SB 962 is an "Unfeasible, counterproductive technology mandate."**
  - **Fact:** CTIA has demonstrated that this is not true by offering to implement this technology in a year, but only on an opt-in basis. Opt-in is not effective, however, because thieves can't tell which phones have the solutions enabled and which do not. This leaves everyone vulnerable to victimization. Furthermore, this technology is already widely available and has been implemented on millions of Apple and Samsung devices.
  - SB 962 will make sure these solutions are on by default by being enabled during activation. Furthermore, the very nature of "opt-out" ensures consumers do have a choice if they wish to not have the theft deterrence feature.
- **Fiction:** "Will not deter theft. Has huge loopholes for pawnbrokers and secondary market sales. A layered approach has shown results in other sectors."
  - **Fact:** In response to the industry we have amended SB 962 to ensure used smartphones developed before the deadline are not caught up in this legislation. Older model phones that are sold peer to peer or through pawn brokers are not covered, and it will take a few years before these older model phones are phased out. We have seen technology prevent crime in the past. For example, when auto theft was on the rise in the 1990's, manufacturers created anti-theft technology which greatly reduced vehicle thefts nationwide. Law enforcement worked hand in hand with manufacturers to harness a technological solution then, preventing crime and victimization. A layered approach was necessary to address automobile theft because the vehicles were being stolen and then stripped for parts. An approach that deterred the theft of automobiles while undermining the ease with which stolen parts could make their way on the market was necessary. For smartphone theft, the ease with which the devices can be readily resold is the major driving factor behind the huge growth in this epidemic. The parts market is a niche market.

- **Fiction:** "Will interfere with emergency services like 911."
  - **Fact:** The bill has been amended to ensure there is no impact on the ability to dial or text 911.
- **Fiction:** "No notice or affirmative consent to "opt in" to tracking technology creates privacy concerns."
  - **Fact:** SB 962 does not have any privacy impacts and does not legislate anything related to geolocation or tracking services. While other manufacturers have deployed their solutions differently, Apple has chosen to couple their existing solution to tracking services, which means consumers can't have the theft deterrent system without having their location tracked. If you turn off location services (Find My iPhone), you turn off the theft deterrent solution. If SB 962 passes successfully it appears that Apple will have to decouple their solution from tracking services, thereby benefiting privacy. This is because in order to be in accordance with FTC guidelines regarding best practices for location tracking users must opt-in to geolocation services. SB 962 requires theft deterrent technology to be opt-out, and accordingly Apple would likely have to decouple their solution from location tracking in order to avoid running afoul of best practices. As a result, there are net positive privacy impacts if this legislation is successful.
  - **Fact:** The very nature of opt-out ensures consumer choice is enshrined in SB 962.
- **Fiction:** "SB 962 is Extremely Overbroad and Ambiguous."
  - **Fact:** Definition of "essential features" has been amended to omit any connection or functionality that is essential to the performance of the solution.
  - **Fact:** Definition of "advanced mobile communications device" has been amended to only include smartphones and tablets.
  - **Fact:** The liability is very clear. If a retailer sells a device manufactured after *** that is not pre-equipped with a solution that meets the criteria specified they are in violation of the law.
  - **Fact:** This law would be enforced just like countless other consumer protection laws are enforced. Prosecuting agencies would seek a civil enforcement action against the retailer in question. Any information that raises suspicion, either through a tip or our own investigation, would enable the prosecutor's office to issue an administrative subpoena. If the devices are being sold without the solutions pre-equipped, we would take action under our civil enforcement powers as specified in this section and unfair business practices. Inspections are determined at random by the Attorney General. On-line sales would be subject to these provisions as well.

SB 962 (Leno)

Principal Co-Author: Assemblymember Skinner
Co-Authors: Senators Wolk, Pavley & Hancock
As Introduced February 6, 2014

Smartphone Theft Prevention

FACT SHEET

SUMMARY

SB 962 will require any smartphone or tablet sold in California to include a technological solution that renders the essential features of the device inoperable when stolen. Such solutions remove the incentive for thieves by eliminating the device's value on the secondary market. As a result, this legislation will go a long way towards ending the epidemic of smartphone theft and ensuring Californians are safeguarded from theft.

BACKGROUND

California is experiencing an epidemic of smartphone thefts, many of which turn violent. The scope of this international epidemic is alarming, and the need for theft deterrence features on mobile devices cannot be understated.

The theft of mobile communications devices now accounts for one third of all robberies in the United States, making it the number one property crime in the country. This trend is reflected in most major cities in California today, with smartphone theft now accounting for over 50% of all robberies in San Francisco and as much as 75% in Oakland. Los Angeles has experienced a 12% increase in this type of crime since 2012. Policing and prosecution are an essential component of crime reduction, but this epidemic is simply too massive and widespread to be addressed by enforcement alone.

With the wireless industry earning an estimated $30 billion annually from lost and stolen devices, the industry lacks motivation to end this epidemic and safeguard Californians. As a result, it is essential that government step in and require the industry to take steps to end this wave of violent thefts and ensure the safety of consumers.

Technological solutions that render stolen devices useless already exist, but the industry has been slow to act. Meanwhile, Consumer Reports estimates that 1.6 million Americans were victims of smartphone theft in 2012. What's worse, news reports indicate that smartphone theft increased again in 2013 in urban centers across the country. With robberies involving mobile communication devices at an all-time high, California cannot stand-by when a solution to the problem is readily available. Manufacturers and carriers have the opportunity to deter

violent crime, eliminate the secondhand market for stolen mobile communications devices, and prevent their customers from becoming the next victim.

SOLUTION

SB 962 requires that all advanced communications devices (smartphones and tablets) sold in California must come pre-equipped with a theft-deterring technological solution that renders the essential functions of the device useless when stolen. The consumer may affirmatively opt-out of using the technological solution, but every device must come pre-equipped and enabled with this technology in order for the deterrent value of the solution to be as effective as possible.

The result will be to remove the re-sale value of stolen devices, thus reducing the current incentive for thieves to prey on smartphone users.

STATUS

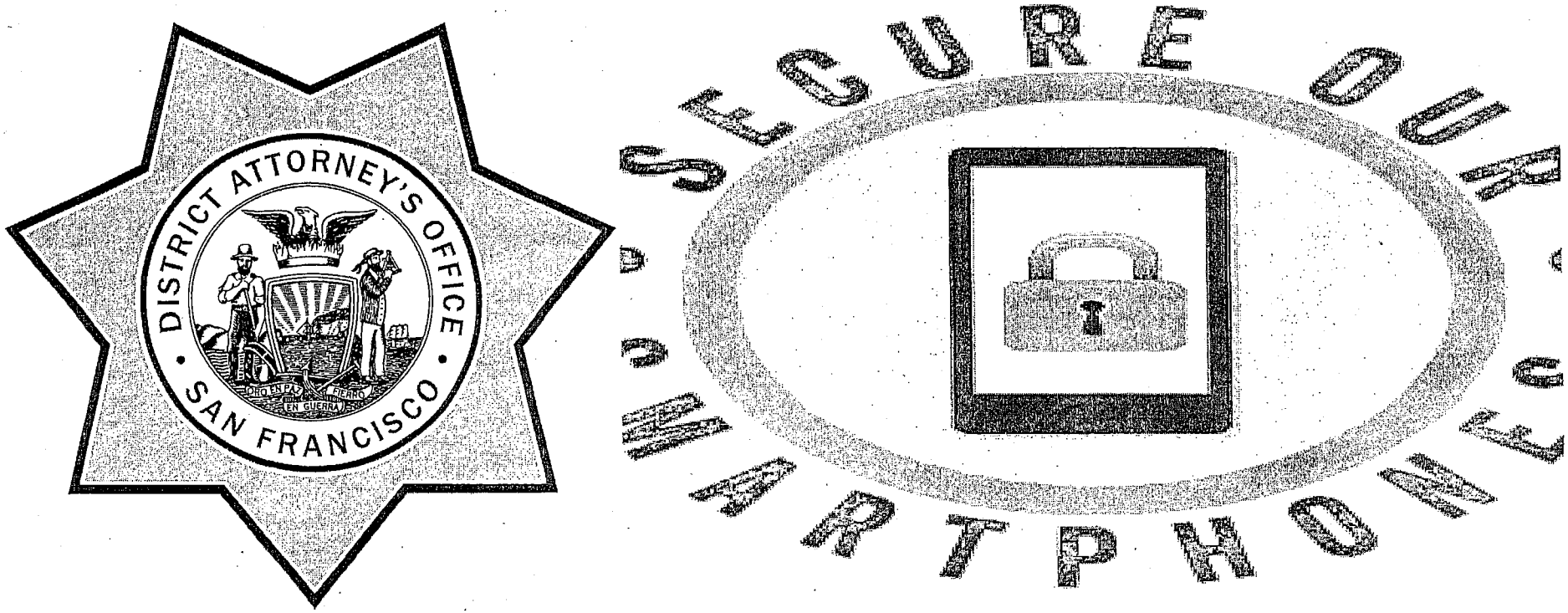
Introduced February 6, 2014

SUPPORT

- San Francisco District Attorney George Gascón (Sponsor)
- Secure Our Smartphones Coalition
- CA Police Chiefs Association
- CA District Attorneys Association
- Los Angeles County Professional Peace Officers Association
- Long Beach Police Officers Association
- Santa Ana Police Officers Association
- Association of Orange County Deputy Sheriffs
- Sacramento County Deputy Sheriffs Association
- California Fraternal Order of Police
- San Francisco Mayor Ed Lee
- San Francisco Police Chief Greg Suhr
- City of Los Angeles
- Los Angeles Mayor Eric Garcetti
- Los Angeles Police Chief Charlie Beck
- City of Oakland
- Oakland Mayor Jean Quan
- Oakland City Council President Pro-Tempore Rebecca Kaplan
- Oakland City Councilman Dan Kalb
- Oakland Police Chief Sean Whent
- Alameda County DA Nancy O'Malley
- The Utility Reform Network
- Consumer Action
- Consumer Federation of California
- Consumers Union
- City of San Diego
- City of Santa Ana
- City of Berkeley
- City of Emeryville
- SF Municipal Transportation Agency
- BART (Bay Area Rapid Transit)
- BART Police
- Neighborhood Crime Prevention Councils of Oakland
- CA Transit Association
- Temescal Merchants Association
- Associated Students of the University of California
- Hayward Police Chief Diane Urban

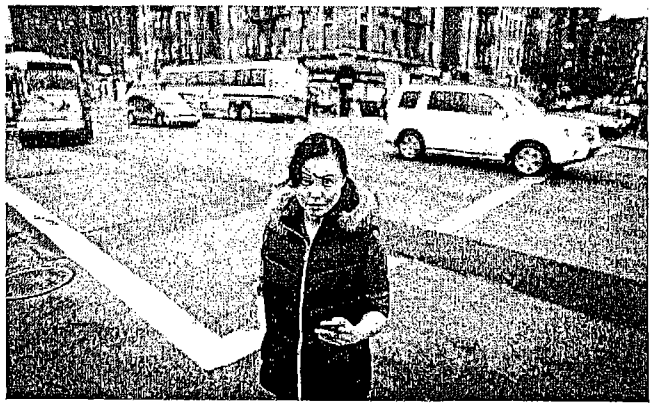
Contact: Daniel Seeman, 916-651-4011
Version: April 7, 2014

San Francisco District Attorney George Gascón
Overview of SB 962
The Smartphone Theft Prevention Act
April 1, 2014

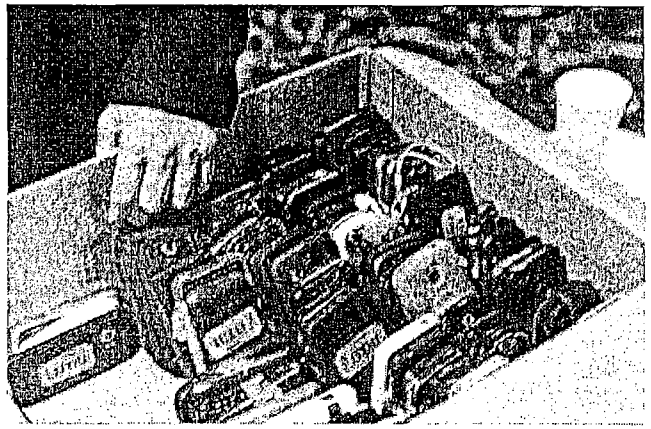


Why Not Increase Enforcement?

- Most robberies now involve the theft of a smartphone.



- In 2012, more than 50% of all robberies in San Francisco involved the theft of a mobile communications device. The number is as high as 75% in Oakland, and this type of crime increased by 12% in Los Angeles just last year.

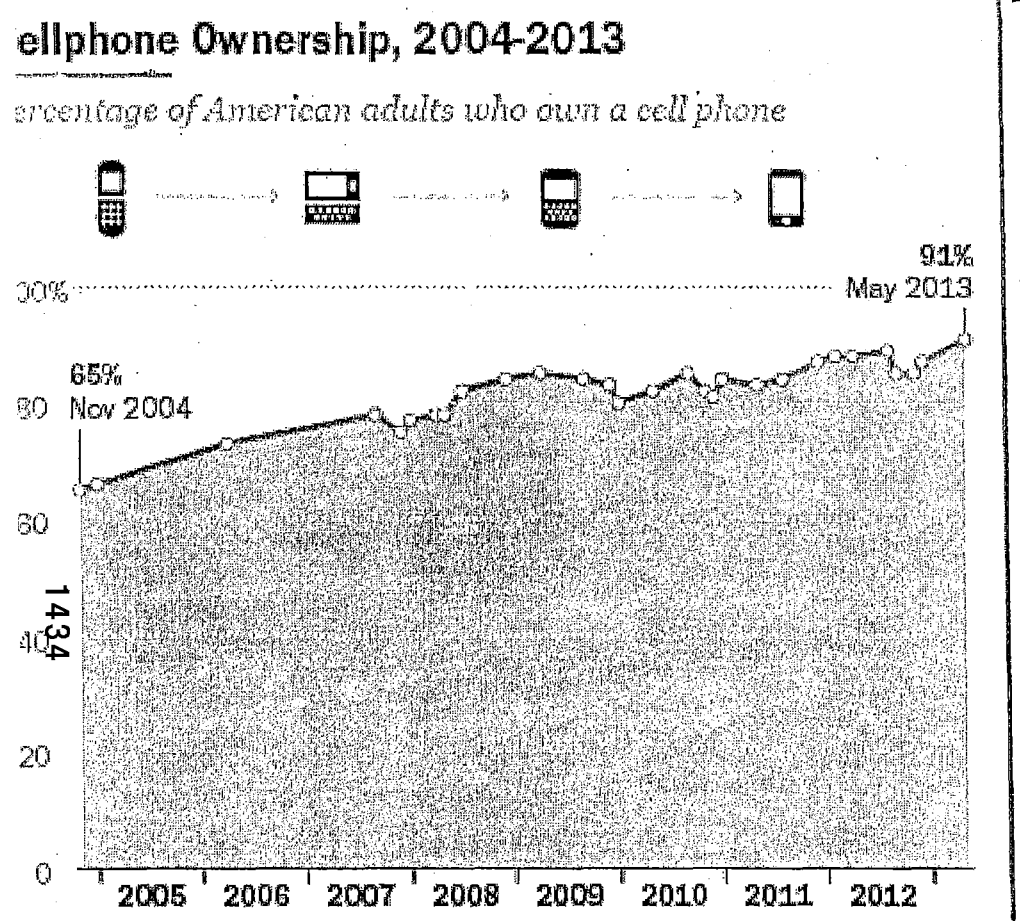


- Trends indicate that this type of crime continues to grow.

- Consumer Reports estimates that 1.6 million Americans were victimized for their smartphones in 2012.

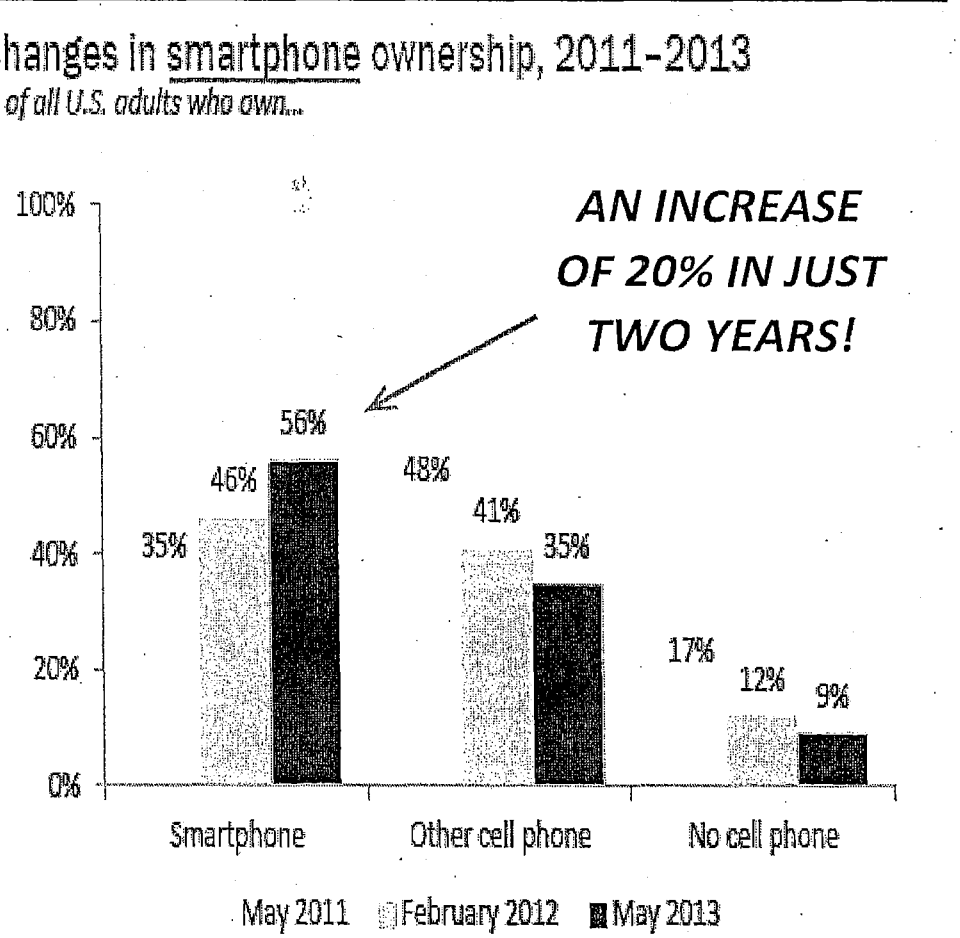
Takeaway: Due to the pervasive nature of the crime, enforcement alone is not an effective strategy.

91% of Americans own a Cellphone, 56% own a Smartphone



urce: Pew Research Center's Internet & American Life Project, April 17-May 19, 013 Tracking Survey. Interviews were conducted in English and Spanish and on ndline and cell phones. Margin of error is +/-2.3 percentage points based on all dults (n=2,252).

EW RESEARCH CENTER



Source: Pew Research Center's Internet & American Life Project April 26-May 22, 2011, January 20-February 19, 2012, and April 17-May 19, 2013 tracking surveys. For 2013 data, n=2,252 adults and survey includes 1,127 cell phone interviews. All surveys include Spanish-language interviews.

More smartphone owners = More targets for thieves

Street-level thieves feed a massive global black market that is so lucrative the South American drug cartels are now trafficking stolen smartphones

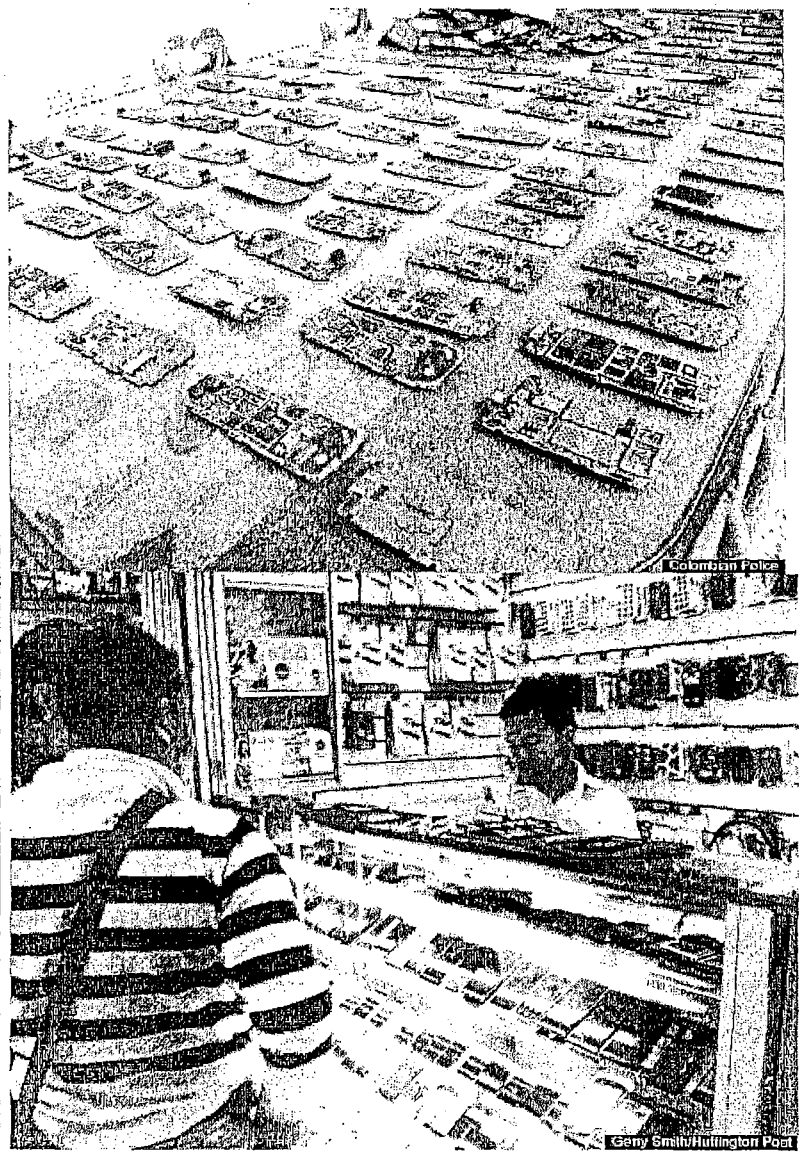
iTHEFT

INSIDE THE GLOBAL BLACK MARKET FOR STOLEN iPHONES

How Stolen Smartphones End Up In The Hands Of Colombian Cartels

Posted: 12/10/2013 4:44 pm EST | Updated: 12/11/2013 11:09 am EST

Recommend Share 1,530 people recommend this. Be the first of your friends.



Despite prevention efforts and Apple's Activation Lock, smartphone theft increased in 2013

- According to the San Francisco Police Department, nearly 2,400 cell phones were stolen in San Francisco in 2013, a 23% rise from the year before.

- New York City police statistics indicate that 8,465 Apple products alone were reported stolen last year, an 8% increase from the year before - it was the second year in a row that thefts of iPhones and iPads went up.

- In Washington D.C., police indicate cell phone thefts increased 6% last year compared to the previous year.

- In D nver, iPhone thefts rose 22% in 2013,

1436

Corporate Responsibility

Is a "kill switch" the answer?

- Wireless consumers are targeted for smart devices because they are easy to steal, valuable, and can be readily resold on the black market.

- Mobile communications device manufacturers and wireless carriers have a responsibility to ensure their customers are not targeted as a result of purchasing their products.

- Smartphone manufacturers and carriers make billions in profits from wireless consumers. They also profit from smartphone theft: Stolen phones must be replaced, and consumers often sign a new one or two year wireless service agreement to purchase new devices at the subsidized rate.

- The implementation of a "kill switch" would render stolen devices inoperable on any network, anywhere in the world. By eliminating the ability for the phone to be reactivated, the value of these mobile communications devices would be equivalent to that of a paperweight. As a result, the incentive to steal them would be eliminated.

- **Several solutions already exist on millions of smartphones around the world. To be effective, however, these solutions must be nearly ubiquitous as thieves can't tell which phones have the solutions enabled and which ones do not. If implemented on virtually all smartphones, there will be a change in behavior as thieves learn they cannot profit from stealing smartphones.**

- We have seen technology prevent crime in the past. When auto theft was on the rise in the 1990's, manufacturers created anti-theft technology which greatly reduced vehicle thefts nationwide.

1437

SAMSUNG

Microsoft

Google

verizon

Sprint

at&t

Ending the Epidemic – SB 962

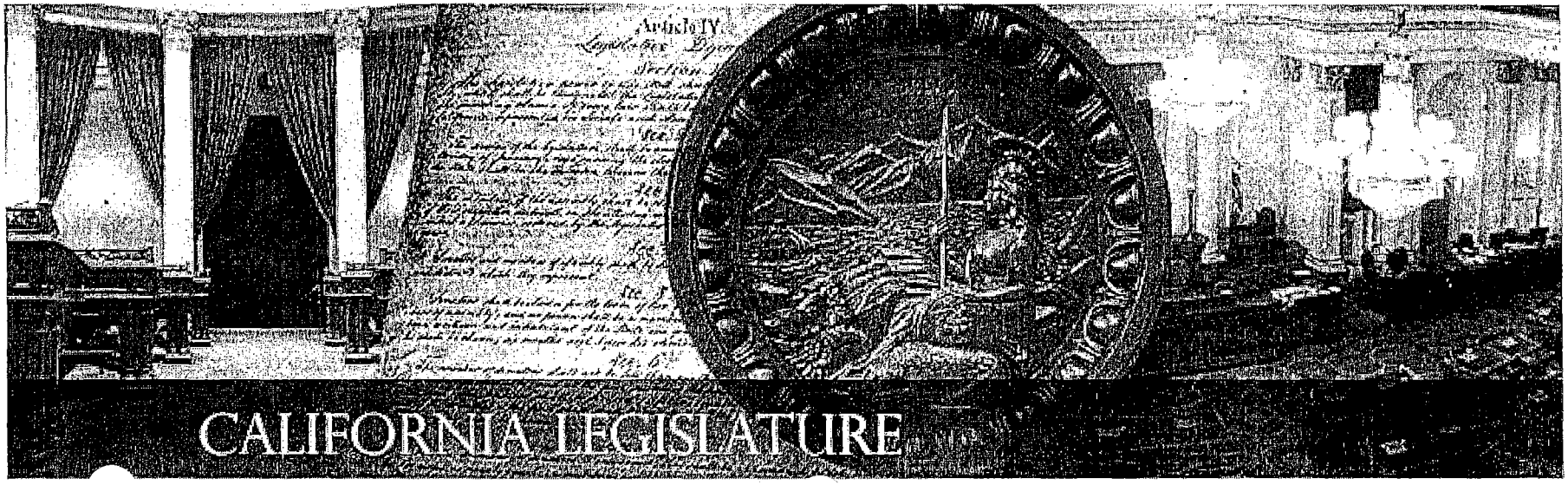
Any smartphone or tablet sold in California after January 1, 2015, shall include a technological solution that has the ability to render the essential features of the device inoperable.

The solution must be able to withstand a "hard reset" or operating system downgrade, and prevent reactivation on a different wireless network without the rightful owner's credentials.

The rightful owner of the device may elect to disable (opt-out of) the solution after sale, and would be able to reverse the solution if the device is recovered.

T438

Any retailer who sells a device without the solution may be subject to a civil penalty.

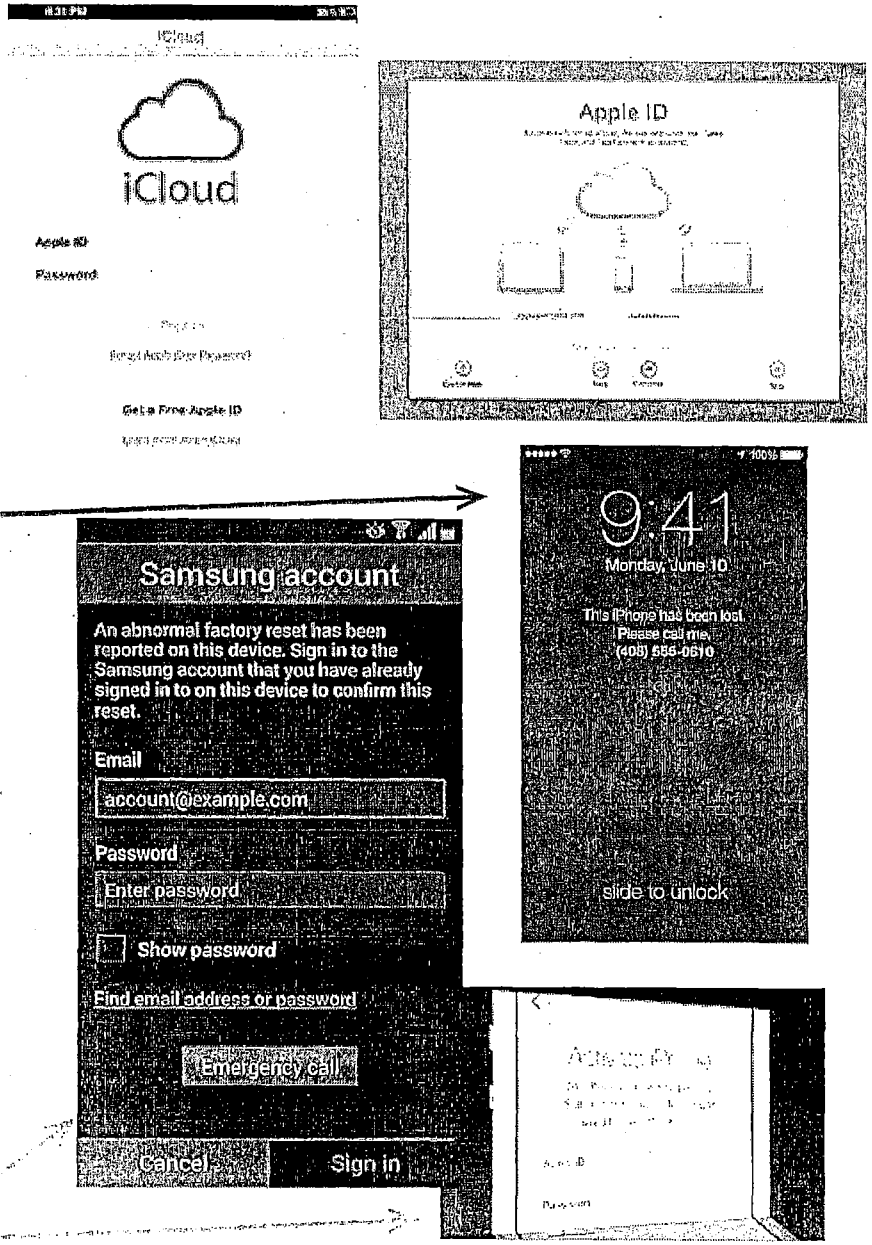


How do these solutions work?

1. Existing solutions require the rightful owner to input credentials such as an email and password when they set up their phone for the first time. This information is stored in "the cloud" along with the identifying information of the device, effectively registering the device to the rightful owner.

2. If the phone is lost or stolen the consumer can login from another device and "brick" their smartphone or tablet, rendering it inoperable.

3. SB 962 goes a step further, however, by not relying on the consumer to take this step. Thieves will typically attempt to restore a smartphone to its default factory settings in order to optimize the value of the device for resale. When they go through the registration process they will need the original owner's credentials to reactivate the device and receive wireless service. This ensures that thieves cannot "wipe" the device and get around the solution, and it protects the right of



Isn't there a stolen smartphone database? Why is that not sufficient?

The existing FCC database has not been effective, and similar databases in countries like the UK have not slowed the epidemic.

The voluntary database established by the wireless carriers does not provide for automatic registration of stolen phones. Under the current system, the burden is on the victim to ensure their device is added to the database.

The database is limited to the big four carriers, AT&T, Sprint, T-Mobile, Verizon, and does not cover any of the smaller carriers.

Most importantly, the database does not cover phones that are stolen and trafficked overseas. With stolen smartphones fetching as much as $2,000 per device abroad, the international trafficking of stolen smartphones is a growing black market that cannot be undermined by the carrier database.

Any expectation that hundreds of international carriers will participate in the database is unrealistic, and such an effort would take many years, subjecting millions of Americans to additional victimization.

Why require the solutions to be "opt-out?"

Existing solutions have not been deployed in a manner which ensures that a majority of smartphones have the feature enabled. Some require the user to download the solution and pay for it, while others require the user to find the option in their settings and turn it on. This means that fewer people have the solution enabled, and fewer consumers have protections in place that prevent their device from being resold on the black market. The real world implication is that if 4 of 5 phones that a thief steals can be resold, the crime is still profitable and the incentive to continue the behavior is intact.

Apple's solution, Activation Lock, is the most widespread "kill switch" type solution to date. Unfortunately, because the security solution is tied to location services, an individual who does not turn on geolocation is never made aware that they don't have the theft deterrence feature enabled. Additionally, if they turn geolocation off, they're not notified that they are disabling the solution.

As evidenced by the increases in smartphone theft in 2013, the solutions have not had high enough adoption rates among wireless consumers to dissuade thieves. Until the vast majority of devices have such solutions enabled by default, everyone is still a target because thieves cannot distinguish between those devices that have the a solution enabled and those that do not. In order to remove the incentive the solution must be enabled on the vast majority of devices, similar to applications like a calculator, flashlight or maps. When this happens, thieves will learn that they can no longer profit from stolen smartphones, and their incentive to engage in the violent behavior will be eliminated.

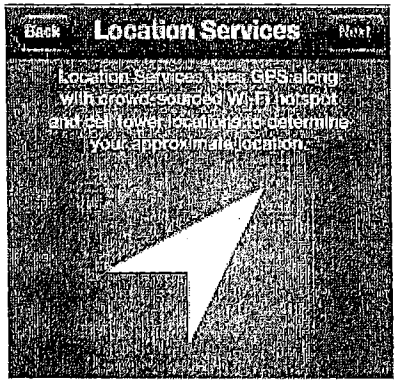
LoJack for Android requires consumers to seek out, pay for and install the solution. This ensures it will never have widespread adoption.

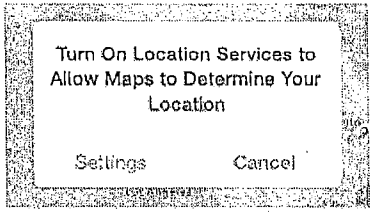
Apple's solution is tied to geolocation and does not provide an indication that the feature is also a theft deterrent system.

Samsung's Reactivation Lock solution is buried in the settings tab. This means consumers have to be aware of the solution and find it before they can turn it on.

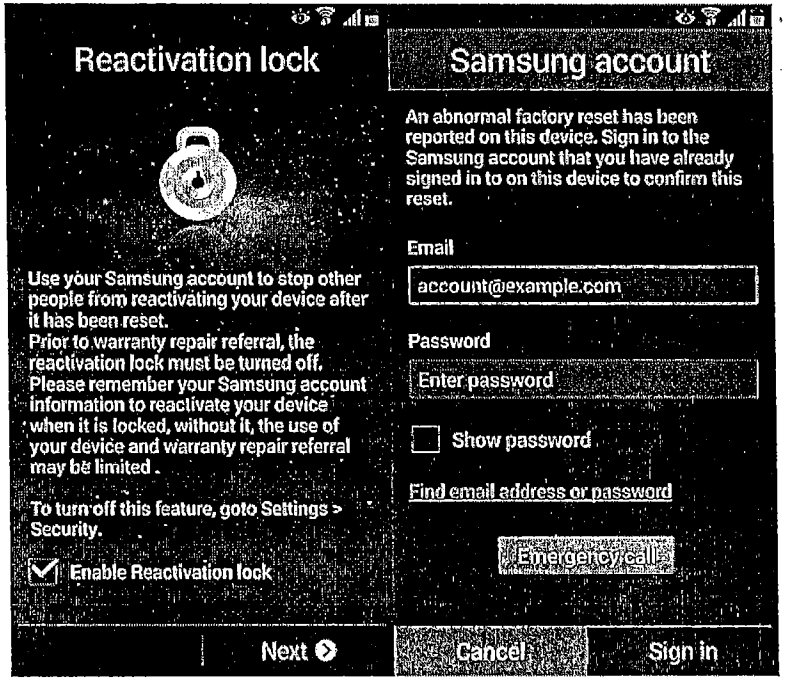
Are There Privacy Concerns Associated with Mandating this Technology?

- No. Nothing in this bill requires these solutions to function in a manner that would raise privacy concerns for consumers. The solutions vary by manufacturer, however, and some existing solutions require geolocation to be enabled for the solution to work.





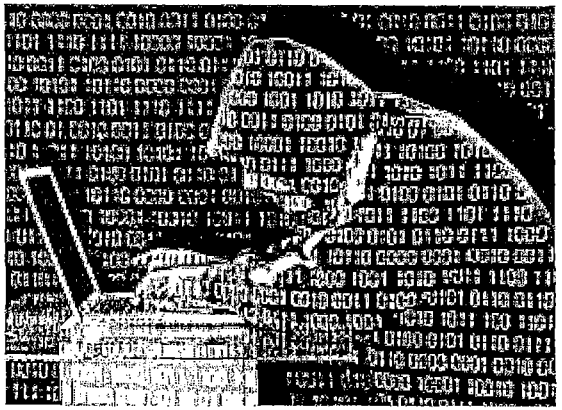
- For example, Apple's existing solution, "Activation Lock," ties the theft deterrent feature to location services. Location services is the ability to track the device's whereabouts to assist with applications like maps.



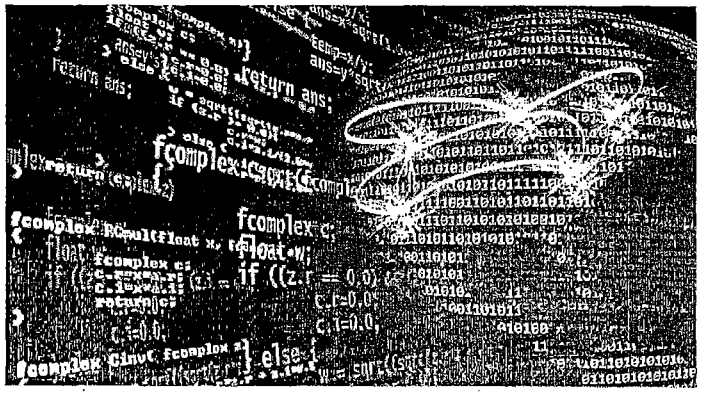
- By contrast, Samsung's "Reactivation Lock" solution is a feature that is kept completely separate from any geolocation services.

Will this bill increase the risk of hacking or cyber-attack?

No, and this is an alarmist argument. The unfortunate reality is that our increased reliance on mobile devices that are connected to the worldwide web means that individuals are at a heightened risk of cyber-attack in their everyday lives. This bill does not change or contribute to that fact; it simply aims to undermine the global epidemic of smartphone theft.

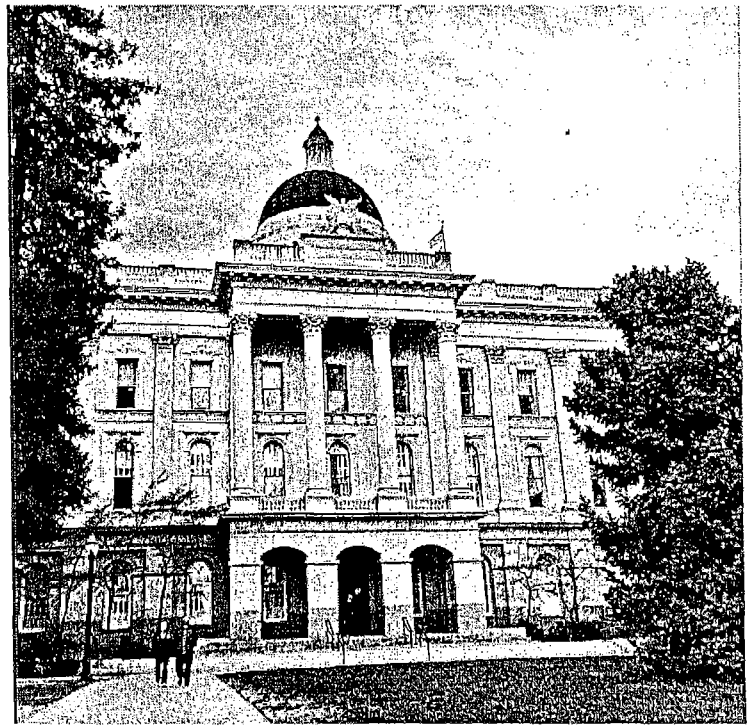


Most importantly, existing theft deterrent solutions that are present on millions of devices around the world have not been "hacked," thus demonstrating the futility of this argument.



Why California State Legislation Instead of Congress?

- Relying on Congress to take action while thousands are victimized every day is irresponsible.
- In the absence of a signed federal bill, we must move forward to protect Californians.
- The legislation being considered in Congress is not opt-out, and is therefore significantly less effective.



Why Do We Need to Legislate This?
Can't the Manufacturers Solve This Problem On Their Own?

While several manufacturers have made meaningful progress, the solutions have not been deployed in an effective manner. Furthermore, most manufacturers have been slow to act, and in some cases the industry has even obstructed progress.

The industry has significant financial disincentives, and we cannot allow profits to drive decisions that have life or death consequences.

Smartphone manufacturers rake in an estimated $30 billion each year due to lost or stolen devices.

&

The top four wireless carriers in the U.S. collect more than $7.8 billion in insurance protection plan premiums.

If required on smartphones nationwide, a kill switch is estimated to cost the industry $2.5 billion on insurance products alone.

THE MAJOR CARRIERS (AT&T, VERIZON, SPRINT, T-MOBILE, & US CELLULAR) REJECTED A TECHNOLOGICAL SOLUTION THAT COULD HAVE SAFEGUARDED THEIR CUSTOMERS

"Carriers Reject a 'Kill Switch' for Preventing Cellphone Theft"

- New York Times, November 19, 2013

"Inside the Hidden Tech Battle Over a Smartphone Kill Switch"

- CBS This Morning, November 19, 2013

"Wireless Carriers Block Simple Solution To Phone Theft To Protect Profits, Prosecutor Says"

- Huffington Post, November 20, 2013

"CARRIERS REJECT KILL SWITCH FOR STOLEN SMARTPHONES"

- Associated Press, November 20, 2013

SB 962

Who thinks manufacturers should implement this technology ubiquitously?

- CA Police Chiefs Association
- CA District Attorneys Association
- San Francisco Mayor Ed Lee
- San Francisco Police Chief Greg Suhr
- City of Los Angeles
- Los Angeles Mayor Eric Garcetti
- Los Angeles Police Chief Charlie Beck
- City of Oakland
- Oakland Mayor Jean Quan
- Oakland City Council President Pro-Tempore Rebecca Kaplan
- Oakland City Councilman Dan Kalb
- Oakland Police Chief Sean Whent
- Alameda County DA Nancy O'Malley
- The Utility Reform Network
- Consumer Action
- Consumer Federation of California
- Consumers Union
- City of San Diego
- City of Santa Ana
- SF Municipal Transportation Agency

What can you do? *Take Action*

1. Support SB 962!
2. Become a co-author.
3. Make sure your constituents are aware of this threat and what steps they can take to protect themselves.
4. Ask your colleagues to support Sen. Leno's smartphone legislation.
5. Join our coalition –add your name to the growing list of law enforcement professionals that support SB 962 and a technological solution to this growing epidemic.
6. Share our change.org petition through your social media channels and email list serves.

Keep in Touch...

DistrictAttorney@sfgov.org

@georgegascon AND @sfdaoffice

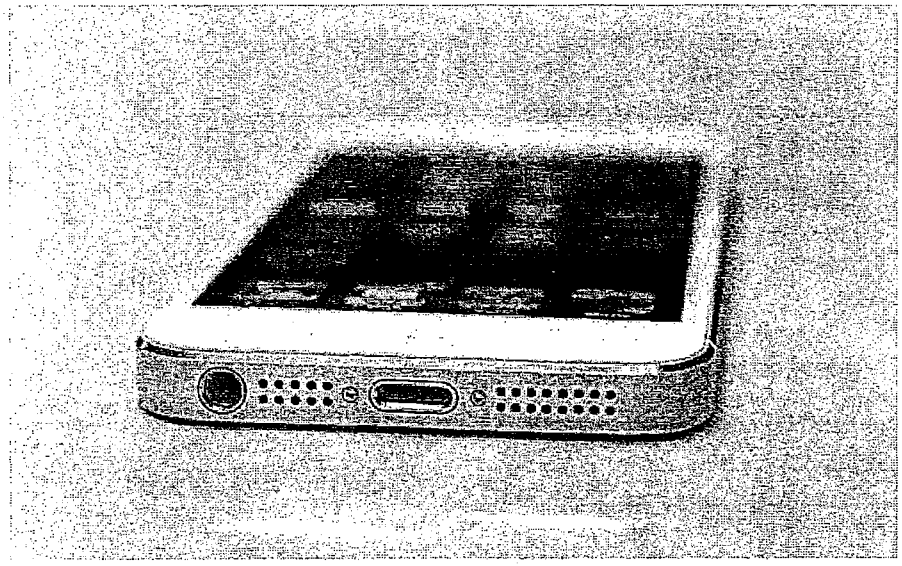
facebook.com/gasconforda

change.org/petitions/secure-our-smartphones

OP-ED

A 'kill switch' to deter smartphone theft: It's the right call

LAPD's chief and San Francisco's district attorney argue that's past time for the industry to act.



The black market for stolen smartphones has become so lucrative that even Colombian drug cartels now traffic in them. (David Paul Morris / Bloomberg / April 22, 2014)

In AT&T's U-verse world, faster may not necessarily be better

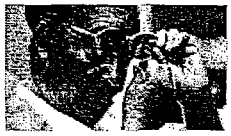
'Haha' and 'LOL': Are texting's

By Charlie Beck and George Gascón
April 22, 2014 | 7:25 p.m.

Do you own a smartphone? If so, you are a target for opportunistic thieves. Robberies and thefts involving smartphones are now the most common property crimes in America. The black market for these stolen devices has become so lucrative that even Colombian drug cartels now traffic in them.

According to a survey by Consumer Reports, some 3.1 million Americans were victims of smartphone theft last year, nearly double the number in 2012. Los Angeles has experienced a more than a 30% increase in smartphone theft

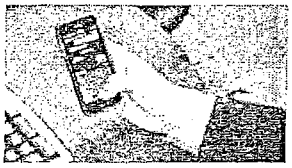
Table set for NBA action on Sterling



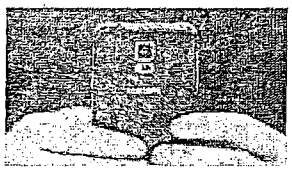
She's homeless and likes it that way

Tony Awards 2014: List of nominees

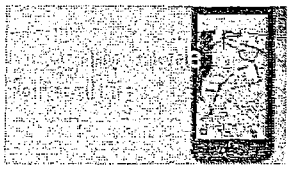
staples simple laziness or signs of social desperation?



Public officials in a wired world: How much privacy should they get?



Whether it's bikes or bytes, teens are teens



Cloak app: For those who want to hide in plain sight

since 2011. The experience can be traumatic, especially when violence is involved. And because people store all sorts of data on their phones, including passwords and credit card information, the ramifications of a theft can extend far beyond the loss of a costly phone and the fear that comes with being victimized.

But this kind of theft, unlike most crimes, has a remarkably simple solution. Cellphone manufacturers and wireless carriers could put an end to the growing number of smartphone thefts by installing and enabling a "kill switch" on all phones. This technology can render stolen devices inoperable on any network, anywhere in the world. Because all smartphones would be useless to anyone but their rightful owners, they would have no resale value, so thieves would have no incentive to steal them.

This technology exists, and it's on millions of smartphones. Unfortunately, it's been deployed in a way that requires smartphone owners to activate it themselves. This is problematic because most smartphone users don't know their devices have the technology or how to turn it on. Moreover, thieves can't tell which phones have the technology enabled and which do not, which leaves everyone vulnerable to victimization.

For nearly 18 months the industry has been pressured to voluntarily implement kill switch technology on all phones in a way that requires consumers to opt out rather than opt in. The idea would be that phones would come already set up with the technology activated. Consumers could opt out if they wanted to, but why would anyone?

The industry has taken some steps in the right direction, but no manufacturers or carriers have fully agreed to what we are urging. It doesn't take much imagination to come up with a plausible reason for their reluctance. Wireless carriers and manufacturers make billions of dollars a year replacing stolen smartphones. They also make money selling theft insurance. Putting an end to smartphone thefts might not be good for business.

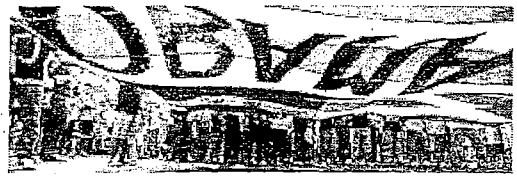
But profits shouldn't be allowed to guide decisions that have life-or-death consequences. In failing to embrace existing technology to safeguard its products, the industry has put its customers in jeopardy. These companies have a responsibility to ensure their customers are not targeted as a result of buying their products.

We can't wait for the industry to grow a conscience when people are getting hurt every day. A bill pending in Sacramento, SB 962 by state Sen. Mark Leno (D-San Francisco), would require smartphones sold in the state not only to have this technology but to have it turned on as the default mode when the phone is purchased. This week, the state Senate will consider the legislation, and you should let your representatives in Sacramento know how you feel on the issue.

Technology has a proven role in preventing crime. When auto theft was on the rise in the 1990s, manufacturers created anti-theft technology that greatly reduced vehicle thefts nationwide. Law enforcement worked hand in hand with manufacturers to harness a technological solution then, preventing crime and victimization. We urge the wireless industry to join us now so we can repeat our previous success and protect wireless consumers everywhere.

Charlie Beck is chief of the Los Angeles Police Department. George Gascón is district attorney of San Francisco.

Ferguson talks about his 'Late Late Show' exit



Photos of the Day

More

Most Viewed Latest News

From three down, one to go for Kings *04/29/2014, 12:01 a.m.*

Penguins hold off Blue Jackets to win series *04/28/2014, 10:53 p.m.*

Gunfire reported amid surveillance operation in Walnut Park *04/28/2014, 10:49 p.m.*

Manu Ginobili helps Spurs even playoff series with Mavericks *04/28/2014, 10:42 p.m.*

Angels surge past Indians, 6-3 *04/28/2014, 10:39 p.m.*

VIDEO

SENATE BILL **No. 962**

Introduced by Senator Leno
(Principal coauthor: Assembly Member Skinner)

February 6, 2014

An act to add Section 22761 to the Business and Professions Code, relating to mobile communications devices.

LEGISLATIVE COUNSEL'S DIGEST

SB 962, as introduced, Leno. Advanced mobile communications devices.

Existing law regulates various business activities and practices, including the sale of telephones.

This bill would require that any advanced mobile communications device, as defined, that is sold in California on or after January 1, 2015, include a technological solution, which may consist of software, hardware, or both software and hardware, that can render inoperable the essential features of the device, as defined, when the device is not in the possession of the rightful owner. The bill would require that the technological solution be able to withstand a hard reset, as defined. The bill would prohibit the sale of an advanced mobile communications device in California without the technological solution being enabled, but would authorize the rightful owner to affirmatively elect to disable the technological solution after sale. The bill would prohibit a provider of commercial mobile radio service, as defined, from including any term or condition in a service contract with an end-use consumer with an address within the state that requires or encourages the consumer or rightful owner to disable the technological solution that renders the consumer's smartphone or other advanced communications device useless if stolen. The bill would make a violation of the bill's requirements subject to a civil penalty of not less than $500, nor more than $2,500, for each violation.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

P2 SECTION 1.

The Legislature finds and declares all of the following:

(a) According to the Federal Communications Commission, one in three robberies in the United States involve the theft of a mobile communications device, making it the number one property crime in the country. Many of these robberies often turn violent with some resulting in the loss of life.

(b) Consumer Reports projects that 1.6 million Americans were victimized for their smartphones in 2012.

(c) According to the New York Times, 113 smartphones are lost or stolen every minute in the United States.

(d) According to the Office of the District Attorney for the City and County of San Francisco, in 2012, more than 50 percent of all robberies in San Francisco involved the theft of a mobile communications device.

(e) Thefts of smartphones in Los Angeles increased 12 percent

in 2012, according to the Los Angeles Police Department.

(f) According to press reports, the international trafficking of stolen smartphones by organized criminal organizations has grown exponentially in recent years because of how profitable the trade has become.

(g) Replacement of lost and stolen mobile communications devices was an estimated thirty-billion-dollar ($30,000,000,000) business in 2012 according to studies conducted by mobile communications security experts. Additionally, industry publications indicate that the four largest providers of commercial mobile radio services made an estimated seven billion eight hundred million dollars ($7,800,000,000) from theft and loss insurance products in 2013.

(h) Technological solutions that render stolen mobile communications devices useless already exist, but the industry has been slow to adopt them.

P3 (i) In order to be effective, these technological solutions need to be ubiquitous, as thieves cannot distinguish between those mobile communications devices that have the solutions enabled and those that do not. As a result, the technological solution should be able to withstand a hard reset or operating system downgrade, and be enabled by default, with consumers being given the option to affirmatively elect to disable this protection.

(j) Manufactures of advanced mobile communications devices and commercial mobile radio service providers have a responsibility to ensure their customers are not targeted as a result of purchasing their products and services.

(k) It is the intent of the Legislature to require all smartphones and other advanced mobile communications devices offered for sale in California to come with a technological solution enabled, in order to deter theft and protect consumers.

(*l*) 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.

SEC. 2.

Section 22761 is added to the Business and Professions Code, to read:

22761.

(a) For purposes of this section, the following terms have the following meanings:

(1) "Advanced mobile communications device" means an electronic device that is regularly hand held when operated that enables the user to engage in voice communications using mobile telephony service, Voice over Internet Protocol, or Internet Protocol enabled service, as those terms are defined in Sections 224.4 and 239 of the Public Utilities Code, and to connect to the Internet, and includes what are commonly known as smartphones and tablets.

(2) "Commercial mobile radio service" means "commercial mobile service," as defined in subsection (d) of Section 332 of Title 47 of the United States Code and as further specified by the Federal Communications Commission in Parts 20, 22, 24, and 25

of Title 47 of the Code of Federal Regulations, and includes "mobile satellite telephone service" and "mobile telephony service," as those terms are defined in Section 224.4 of the Public Utilities Code.

(3) "Essential features" of an advanced mobile communications device include the ability to use the device for voice communications and the ability to connect to the Internet, including the ability to access and use mobile software applications commonly known as "apps."

(4) "Hard reset" means the restoration of an advanced mobile communications device to the state it was in when it left the factory, and refers to any act of returning a device to that state, including processes commonly termed a factory reset or master reset.

(5) "Sold in California" means that the advanced mobile communications device is sold at retail, and not for resale, from a location within the state, or the advanced mobile communications device is sold and shipped to an end-use consumer at an address within the state.

(b) (1) Any advanced mobile communications device that is sold in California on or after January 1, 2015, shall include a technological solution that can render the essential features of the device inoperable when the device is not in the possession of the rightful owner. A technological solution may consist of software, hardware, or a combination of both software and hardware, but shall be able to withstand a hard reset. No advanced mobile communications device may be sold in California without the technological solution enabled.

(2) 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 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.

(c) A provider of commercial mobile radio service shall not include a term or condition in a service contract with an end-use consumer with an address within the state that requires or encourages the consumer or rightful owner to disable the technological solution that renders the consumer's smartphone or other advanced communications device useless if stolen.

(d) (1) A person or retail entity selling an advanced communications device in California in violation of subdivision (b) shall be subject to a civil penalty of not less than five hundred dollars ($500), nor more than two thousand five hundred dollars ($2,500), per device sold in California.

(2) A provider of commercial mobile radio service that includes a term or condition in a service contract with an end-use consumer with an address within the state in violation of subdivision (c) shall be subject to a civil penalty of not less than five hundred dollars ($500), nor more than two thousand five hundred dollars ($2,500), per service contract with an end-use consumer with an address within California.

Print Form

Introduction Form

By a Member of the Board of Supervisors or the Mayor

Time stamp
or meeting date

I hereby submit the following item for introduction (select only one):

☒ 1. For reference to Committee. (An Ordinance, Resolution, Motion, or Charter Amendment)

☐ 2. Request for next printed agenda Without Reference to Committee.

☐ 3. Request for hearing on a subject matter at Committee.

☐ 4. Request for letter beginning "Supervisor [ ] inquires"

☐ 5. City Attorney request.

☐ 6. Call File No. [ ] from Committee.

☐ 7. Budget Analyst request (attach written motion).

☐ 8. Substitute Legislation File No. [ ]

☐ 9. Reactivate File No. [ ]

☐ 10. Question(s) submitted for Mayoral Appearance before the BOS on [ ]

Please check the appropriate boxes. The proposed legislation should be forwarded to the following:

☐ Small Business Commission ☐ Youth Commission ☐ Ethics Commission

☐ Planning Commission ☐ Building Inspection Commission

Note: For the Imperative Agenda (a resolution not on the printed agenda), use a Imperative Form.

Sponsor(s):

Supervisor David Chiu, Mar

Subject:

Supporting SB 962, the Smartphone Theft Prevention Act, to require the installation of a theft-deterring technological solution on smartphones or tablets sold in the State of California

The text is listed below or attached:

Signature of Sponsoring Supervisor: David Chiu

For Clerk's Use Only:

140449