Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP)

Version 1.0

4 December 2014

Table of Contents

Executive Summary

Mobile device and specifically smartphone theft has been identified as a major issue facing consumers, law enforcement and the mobile device ecosystem. The Chairman of the Federal Communications Commission (FCC) requested the FCC Technological Advisory Council (TAC) to create a Mobile Device Theft Prevention (MDTP) Working Group in order to explore the widespread problem of mobile device thefts and to develop recommendations for the FCC by the end of 2014 to mitigate mobile device theft. The MDTP Working Group evaluated the device theft problem, existing solutions addressing device theft and the gaps between the problem and existing solutions with a focus on issues such as cybersecurity, privacy and outreach needs. The MDTP Working Group brings stakeholders with widely different areas of focus and expertise to work together to begin to define a national mobile theft deterrent strategy and associated implementation plan to protect consumers.

The scope of this report is the theft of smartphones. Any references to mobile devices, mobile phones, cellular phones in this report can be considered to be a reference to smartphones.

Highlights of the group's findings include:

- There are no current official national or international smartphone theft statistics. The industry's database has only been operational in the U.S. for the past few years, is not fully subscribed to by all the carriers especially on a global basis, and is not widely used or known about especially by law enforcement. The large number of law enforcement agencies in this country (approximately 18,000 according to the results of the Census of State and Local Law Enforcement Agencies conducted by the Bureau of Justice Statistics) makes the aggregation of mobile device theft data from law enforcement agencies a significant challenge.
- The MDTP Working Group was pleased to obtain preliminary data from 21 police jurisdictions with a population of over 19.7 million indicated the 2013 phone theft rate of 368.9 phone thefts per 100,000 individuals. This figure is about 2.7 times fewer than 3.1 million thefts that have been widely reported in Consumer Reports surveys[1]. In any case, the number of thefts is quite considerably exceeding one million thefts per year. To position this number, collected law enforcement data combined with FBI crime data would estimate that for 2013 at least one tenth of all thefts and robberies committed in the US are associated with the theft of a mobile device. As a caveat, there is considerable concern that the reported theft rate may be under reported, especially in cities that have not established a law enforcement focus on this criminal activity area. The more troubling issue at this point is that it challenging to obtain and analyze the data; thus there is insufficient data to determine the extent and trend of criminal activity.
- More troubling than the data limitations is that fact that the Mobile Device Theft Working Group was unable to obtain any definitive information on the destination of the millions of stolen smartphones. Anecdotal information seems to strongly suggest that at least a subset of the stolen smartphones are being exported from the United States to countries that are both geographically and politically remote from the U.S. This underscores that fact that smartphone theft is an international issue which will ultimately require multi-national coordination. Especially given this point, it is important that the FCC provide national leadership in addressing this critical global issue.

[1] http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

- On the positive side, industry groups (e.g., CTIA, GSMA-NA) have developed voluntary commitments and best practices on smartphone theft mitigation that can be adopted by individual members. However, not all relevant stakeholder groups have adopted these voluntary commitments or best practices. Meaningful theft voluntary commitments or best practices should be in place among all such groups both to better identify pragmatic steps that should be taken as well as to incentivize implementation of effective measures. Further, given the evolving nature of the issue, these voluntary commitments and best practices need to be regularly reviewed and enhanced to be effective.
- A significant number of technology based initiatives that applied together can be of significant assistance, especially when introduced in the context of a broader set of initiatives. Over the past few years, great strides forward have occurred regarding technology methods to reduce phone theft via solutions voluntarily rolled out by carriers, OS providers, manufacturers and third party vendors. This is a very good start and there is some evidence it is impacting criminal activity even today. Looking forward, the MDTP Working Group found that there is no single technology "silver bullet" that will eliminate phone theft and therefore a complementary suite of technical and operational mitigation techniques will need to be made available and applied to gain additional impact to this issue.
- Establish a common national framework for smartphone anti-theft measures that considers all stakeholders and input from all parties involved and explore the basis for preemption. The goal of this framework is to prevent conflicting or growing requirements that may impact the ability of the industry to deliver solutions uniformly to consumers in the United States and US territories in a timely manner. This framework will need to be enhanced on a continued basis.
- Initiatives are needed to improve:
  - The efficient blocking of stolen devices on individual networks depends on technology that ensures the secure implementation of unique device identifiers (e.g., IMEIs, MEIDs) on all smartphones. For example, the world's leading GSM/LTE device manufacturers agreed to support a range of measures to strengthen IMEI security[2] to provide confidence in device blocking and the deployment of enabling technologies and progress is monitored by the GSMA. While all smartphones sold in reputable US retail environments support this set of measures, unfortunately, in a global market not all smartphones have this hardening at this time and not all manufacturers have subscribed to this set of measures. Additionally, counterfeiters can impersonate legitimate smartphones.
  - Additional operators must to be encouraged to participate in the April 10, 2012 CTIA Smartphone Anti-Theft Voluntary Commitment[3] to take certain networked based actions (e.g., GSMA IMEI Database) to help law enforcement deter smartphone theft. In turn the database must be made more widely known to law enforcement and other stakeholders to ensure its effectiveness and widespread use.
  - Data collection will be key to understand if measures being implemented are effective and being utilized. Data collection will also help provide insight into understanding of the consumer actions to deploy smartphone anti-theft tools and techniques along with

[2] http://www.gsma.com/publicpolicy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf.

[3] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

the hoped for understanding of what criminals are doing with stolen smartphones. The GSM Association's North American Regional Interest Group, along with other appropriate stakeholders, should develop a best practices and guidelines on how to measure and report on network-based blacklisted devices going forward, including guidelines to establish consensus in terms of blacklisting policies to ensure consistency of what is blocked and measured.

- Ensure law enforcement have better understanding of anti-theft tools available to aid theft investigations, and the provision of more easily used and understood anti-theft tools for law enforcement will be a critical component of the solution going forward.
- Broad consumer adoption of phone theft deterrent measures is important to reducing phone theft. Therefore the efficient and effective education of consumers on phone theft and technology methods including device based solutions to remotely lock/locate/erase data from smartphones and about the ability to secure/lock smartphones with passwords must be enhanced. This is a critical shared responsibility of all stakeholders, including law enforcement, the carriers, and the device providers.

The MDTP Working Group agrees that the top priority recommendations presented in this report represent the most promising short-term actions the FCC and other stakeholders can undertake to have an impact on smartphone theft. The MDTP Working Group has also provided additional recommendations that should be undertaken by industry and law enforcement; there are also recommendations regarding continuing work for the FCC TAC.

1 Overview

This overview section provides the report introduction, the mission statement, the methodology for the development of the report, the membership of the Mobile Device Theft Prevention (MDTP) Working Group, and the structure of the report.

1.1 Introduction

The Federal Communications Commission (FCC) Technological Advisory Council (TAC) created the MDTP Working Group in order to explore the widespread problem of mobile device thefts and to develop industry-wide recommendations for the FCC by the end of 2014 to mitigate mobile device theft.

Americans rely daily on mobile devices not only for traditional voice and text communications, but also as essential gateways to the Internet for browsing the data they need and as repositories for personal and business information. As a result, mobile device theft is a significant concern. Mobile device thefts can impose personal, physical, and financial harm on consumers.

Mobile device theft is a complex issue that is present on both local and global levels. It can be perpetrated as a "crime of opportunity," as well as part of a larger criminal enterprise. Opportunistic thieves may use a stolen device as their own personal media devices (e.g., camera, music player, Wi-Fi device), or sell the stolen device locally or online for "quick cash." On the other hand, devices that are stolen as part of a larger criminal enterprise may be quickly shipped out of the country. The stolen devices, or parts thereof (e.g., battery, displays, memory), may then be resold (with or without cellular capability) in areas of high demand; SIM cards may be exploited to perpetrate roaming fraud; and personal identifying information on the devices may be utilized to facilitate identity theft or other fraudulent activities.

Law enforcement entities may be hindered by a lack of data, by a lack of access to data, and by the sheer number of device thefts that occur. Current stolen device databases pertaining to different technologies may not be complete, are not integrated, and not easily accessible or widely known to most law enforcement entities. Associated problems will be explored in the body of this report. Consumer awareness is also an issue.

1.2 Mission Statement

The TAC Mobile Device Theft Prevention Working Group, to fulfill its charge of exploring the problem of mobile device theft and developing industry-wide recommendations for the FCC to deter and mitigate mobile device theft, should (1) define key terms that are central to this matter; (2) develop best practices for consumer engagement and education; (3) explore stakeholder coordination and data sharing; (4) ensure appropriate considerations of cybersecurity concerns; (5) identify gaps with existing solutions; (6) analyze the potential necessity and value of new technical and operational solutions to deter thefts and enable the recovery of stolen devices; and (7) identify standards organizations and industry fora to implement solutions. The Working Group has the opportunity to bring together diverse perspectives to analyze the problem and provide recommendations that address the unique scale of mobile device theft.

1.3 Scope

The scope of this report has purposefully been limited to the theft of smartphones since smartphones are by far the largest component of the problem and is sufficient complex as a topic of focus. Any references to mobile devices, mobile phones, cellular phones in this report can be considered to be a reference to smartphones.

1.4 Methodology

In order to develop this report within the project timeline, the MDTP Working Group established five subgroups to focus on various aspects of the mobile device theft problem. These five subgroups are identified in the following figure:

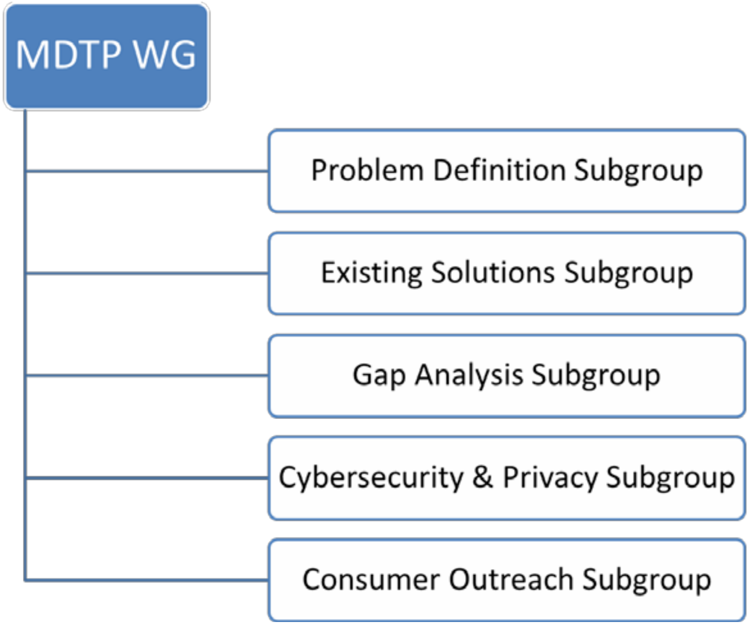

MDTP WG
Problem Definition Subgroup
Existing Solutions Subgroup
Gap Analysis Subgroup
Cybersecurity & Privacy Subgroup
Consumer Outreach Subgroup

Figure 1: MDTP Working Group Structure

Each subgroup was responsible to research their specific topic and to develop report content including recommendations, if applicable. The results of the research of each subgroup are provided as separate sections in this report. The recommendations from all subgroups are consolidated into one set of recommendations which are provided in Section 8.

The responsibilities assigned to each subgroup are summarized in the following table:

Table 1: MDTP Subgroup Responsibilities

Subgroup	Responsibilities
Problem Definition	Documentation of the Mobile Theft problems & issues consistent with FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. These will include: • Definition of terms; • Identification of scope, scale for MDTP current challenges; • Identification of challenges positioned from various stakeholders.
Existing Solutions	Deliver high-level representations of existing and pending solution components from across the globe; identify capabilities and impacts as they associate to the “aspirational” Consumer Response Flow (See Figure 3).

Subgroup	Responsibilities
Gap Analysis	Determine what is needed to move from the current state to the desired future state of mobile device theft prevention. This will include: • Identification of desired outcomes; • Identification of existing practices; • Identification of gaps.
Cybersecurity & Privacy	Address cybersecurity and privacy issues consistent with FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. These will include: • Definition of terms; • Identification of threats and vulnerabilities for MDTP solutions; • Use cases to illustrate the threats and vulnerabilities; • Identification of mitigation strategies, existing or new; • Use cases to illustrate how the mitigation strategies may be applied; and • Identify standards organizations and industry venues that are relevant to the development of best practices.
Consumer Outreach	Consider and develop best practices for consumer engagement and education that are consistent with the FCC Technological Advisory Council as it relates to Mobile Device Theft Prevention tools and solutions. The steps taken will include: • Definition of terms; • Identification of current industry efforts and gaps; • Understanding consumer behavior regarding reporting thefts and use of anti-theft solutions; • Identification and review of best practices for similar types of consumer engagement and education programs; • Identification of key stakeholders and industry fora that are relevant to the development and implementation of best practices.

1.5 MDTP Working Group Membership

Table 2: MDTP Working Group Membership

Name	Organization
Brian K. Daly, Co-Chair	AT&T

Name	Organization
Robert Kubik, Co-Chair	Samsung
Asaf Askenazi	Qualcomm
Jay Barbour	Blackberry
Chris Bender	Motorola Mobility
Alan Bersin	Department of Homeland Security (DHS)
Bradley Blanken	Competitive Carriers Association (CCA)
Craig Boswell	Hobi
Jeff Brannigan	Department of Homeland Security (DHS)
Chris Drake	iconectiv
Eric Feldman	ICE/Homeland Security Investigations
John Foust	Metropolitan Police, Washington, DC
Les Gray	Recipero
Jamie Hastings	CTIA
Joseph Heaps	Department of Justice (DOJ), National Institute of Justice
Gary Jones	T-Mobile USA
Benjamin Katz	Gazelle
Sang Kim	LG
Jake Laperruque	Center for Democracy and Technology (CDT)
Iren Liu	Lookout
John Marinho	CTIA
Samuel Messinger	US Secret Service
James Moran	GSM Association
Jason Novak	Apple
Kirthika Parmeswaran	iconectiv
Greg Post	Recipero
Dennis Roberson (TAC Chair)	Illinois Institute of Technology
Ian Robertson	Motorola Mobility
Deepti Rohatgi	Lookout
Mark Romer	Asurion
Mike Rou	ebay
Matt Rowe	Gazelle

Name	Organization
Christian Schorle	FBI
Ron Schneirson	Sprint
David Strumwasser	Verizon Wireless
Maxwell Szabo	City and County of San Francisco
Nick Tucker	Microsoft
Samir Vaidya	Verizon Wireless
Aya Yogev	Lookout

Also, DeWayne Sennett of AT&T served as Document Editor and Document Manager for the development of this FCC TAC MDTP report.

1.6 Structure of Report

This report is structured as follows:

- Section 1 contains the report overview including the introduction, the mission statement, the scope of the report, a description of the methodology used to develop this report, the MDTP Working Group membership, and the structure of this report.
- Section 2 describes the current and aspirations flows as related to mobile device theft.
- Section 3 contains the findings of the Problem Definition subgroup.
- Section 4 contains a summary of the findings of the Existing Solutions subgroup.
- Section 5 contains the findings of the Gap Analysis subgroup.
- Section 6 contains the findings of the Cybersecurity and Privacy subgroup.
- Section 7 contains the findings of the Consumer Outreach subgroup.
- Section 8 contains the consolidated recommendations for the FCC, for law enforcement, for the industry, and for further work activities.
- Appendix A contains a glossary of the terms used in this report.
- Appendix B contains the Minnesota State Law.
- Appendix C contains the California State Law.
- Appendix D contains the detailed finding of the Existing Solutions subgroup.

2 Current and Aspirational Mobile Device Theft Flows

The MDTP Working Group initially considered the following two diagrams which portray the current mobile device theft flow and a potential aspirational mobile device theft flow. Each figure starts with a triggering event of a smartphone being stolen and the chart indicates scenarios with variable time intervals after the smartphone theft. Ideally, the consumer response will occur as soon as possible after the triggering event.

The major difference between the current flow and the potential aspiration flow paths is the greater use of methods for law enforcement, carriers, insurers, consumer and resellers to be able to confirm if a device has been stolen. In addition the potential aspiration flow path would also include methods for increased reporting and better information sharing between various touch points of the mobile device ecosystem. Detailed recommendations towards achieving this aspiration view are found in Section 8.

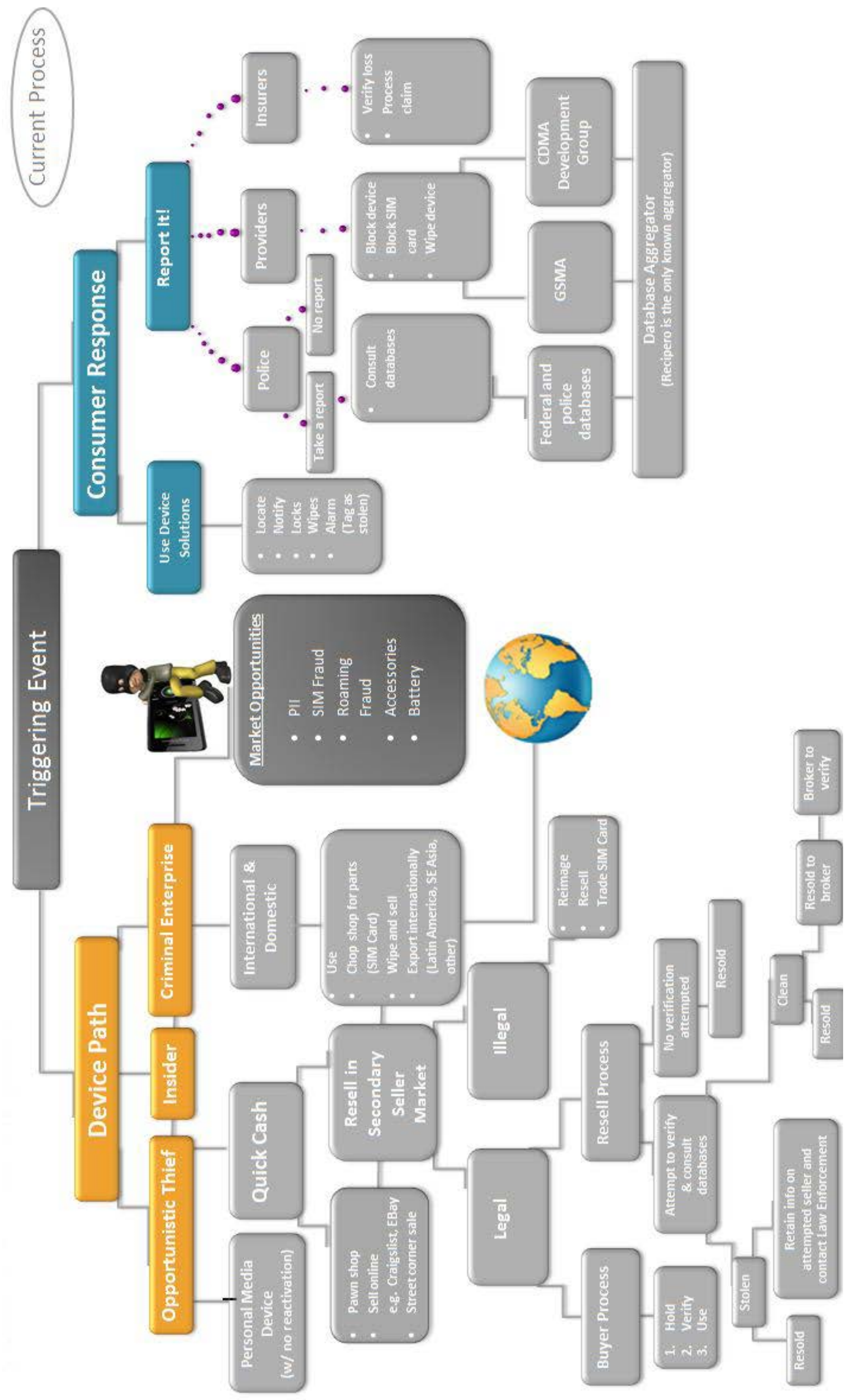


Figure 2: Smartphone Theft Current View of Events

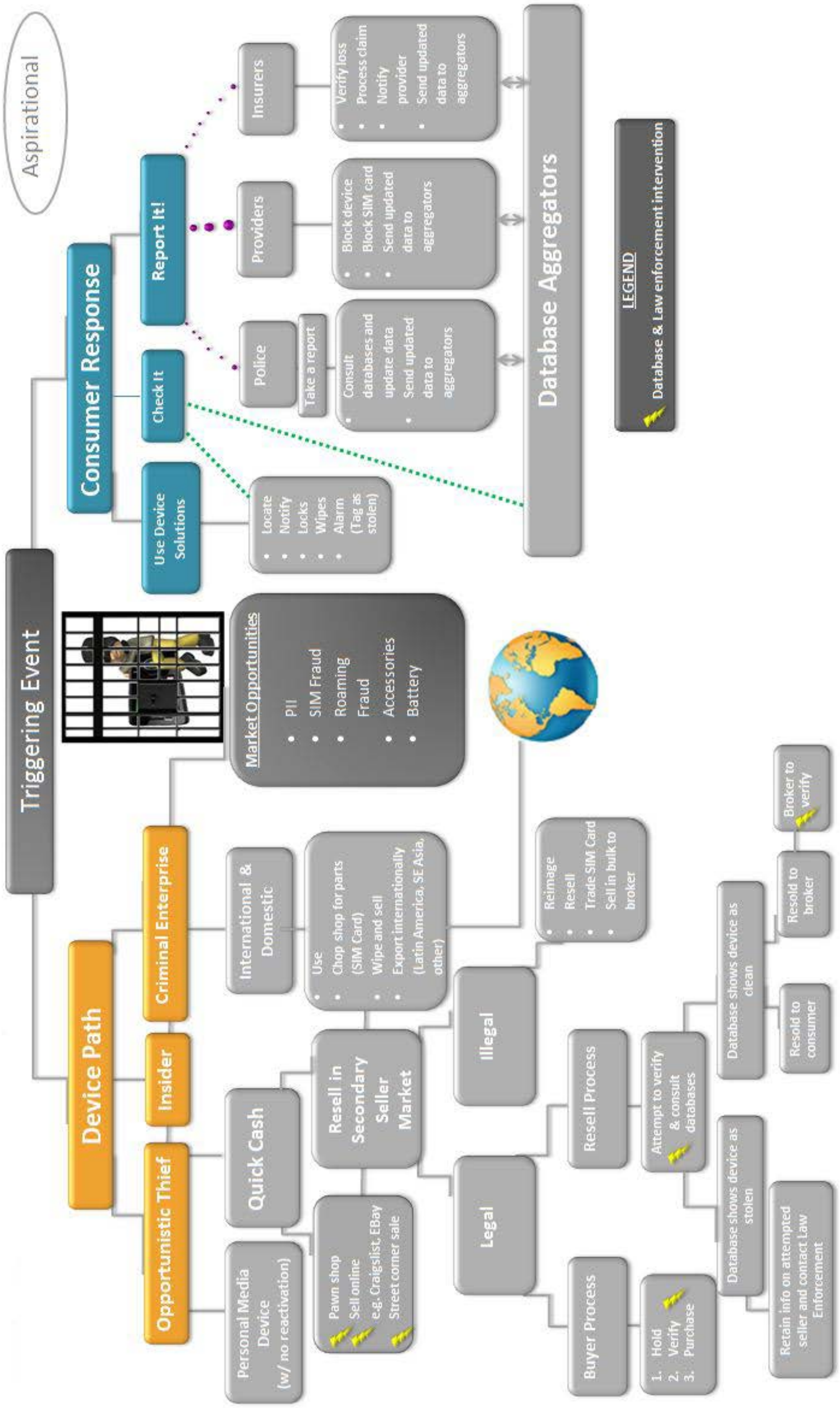


Figure 3: Smartphone Theft Aspirational View of Events

3 Problem Definition

This section provides information defining the mobile device theft problem and is organized into the following subsections:

- Criminal Activities
- Mobile Device Theft Statistics
- Mobile Device Information
- Industry Policies
- Laws – State and Federal
- Device Owner Reaction to Mobile Device Theft
- Other Stakeholder Response to Mobile Device Theft

3.1 Criminal Activities

3.1.1 Theft Definition

> **Definition of Theft:** This definition is consistent with most developed judicial systems "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it".

It can be inferred from this definition that any entity permanently deprived of their property dishonestly by another is a victim of theft.

It should also be inferred that since fraud is a dishonest act then devices appropriated by fraud must also render their owners a victim of theft.

These are not complex legal arguments. They are simple principles rooted in common sense that should be recognized.

When considering the definition of the subworking group's problem then, the subworking group has been careful not to narrow its perception to that of the consumer as the only victim. Any legal entity, whether personal or corporation, may be a victim of theft.

Finally, the subgroup must consider fraudulent activities in its scope as it follows from the above principles that processes ending in theft may begin with a fraud. Indeed, one may argue that what begins with fraud may inevitably end in theft.

With the above scope in mind, a few examples of theft that comprise the problem, the subworking group seeks to address are;

1. A member of the public is a victim of burglary, snatch, assault etc. They are the victim of theft.
2. An individual sells a device given to them by their employer and reports to the employer that it was lost or stolen. The employer is a victim of theft.
3. An individual leases a device such as contract lease or lease purchase and sells the device without the lessor's permission. In this case the lessor is a victim of theft and the person who buys the device in good faith is a victim of deception.

4. An individual makes a false insurance claim for a device. Upon fulfillment of the claim, legal title passes to the insurer. If the device is sold on, whether by the claimant or a finder, the insurer becomes a victim of theft.

There are hundreds of variations on the examples above but these represent a core. It should also be recognized that the cost to society of crimes related to the above activities is much greater than the value of the device that is the subject of the theft.

- Insurance fraud drives up claims settlement costs and premiums.
- False reporting to the police inflates recorded crime statistics while at the same time drawing resources away from the investigation of genuine crimes.
- Stolen devices are traded internationally depriving nations of tax income that would otherwise come from the movement of legitimate devices.
- Attempts to circumvent device blocking by using illegitimate tools to change device identities can have unintended consequences on devices and cause them to operate in undesirable and unpredictable ways.

3.1.2 Consumer Theft

The majority of these are snatch and grabs in public places.[4] With these numbers, a multilayered solution is most likely to be effective. Effective solutions must deter the criminal. This means that solutions must be difficult to defeat and widely deployed. In addition, the ‘utility window’ for the stolen devices or value to the thief must be very small. Those involved in the stolen device ecosystem must expect the device to lose its value almost immediately following the theft and that consumers will be reluctant to buy devices from unknown and untrusted sources because of the likelihood that these devices will cease to operate within a short timeframe.

Snatch and grab thefts may present a further challenge in that the phone may be more likely to be unlocked at this time since the consumer was presumably using it. Handset based anti-theft features therefore must not be easily de-activated in this mode and still be effective if later engaged by the consumer or authorities. The consumer should be capable of utilizing anti-theft features after the mobile device may have been stolen (e.g., consumer can remotely lock their phone). These same anti-theft features should have easily reversible and fully authenticated options in the event the owner “finds” a device initially suspected of being stolen.

Current experience indicates that a minority of users take advantage of anti-theft features on phones (e.g., PIN lock, “Find my phone”, etc.) Users can activate a device but opt-out of activating deterrent features. Such anti-theft capabilities should be a basic part of the activation process. It should be made clear to the consumer that activation of these features is an anti-theft deterrent. Solution providers should provide the capability to opt-out of these services and

[4] Based on a study reported by Lookout, titled Phone Theft in America (https://www.lookout.com/resources/reports/phone-theft-in-america), nearly half (44%) of the victims in the study had forgotten them in a public setting, 14% of smartphones were taken from a car or a house that was burglarized, and 11% of the victims had the smartphone stolen off their person. Additionally, reports in the UK have highlighted this scenario as the common strategy used by thieves. (Reducing Mobile Phone Theft and Improving Security, released 9/11/2014 and provides a detailed look at the crime statistics, victim demographics, and trends of mobile phone theft in the UK https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351135/HO_Mobile_theft_paper_050914_FINAL.PDF).

strong standardized instruction should be included to the consumer about the risks of opting out of these capabilities.

Longer term, greater emphasis should be placed on lowering the barriers to consumers utilizing such features. These might include simpler interfaces to activate protection features, e.g., fingerprint, facial recognition; or addressing other user concerns such as privacy. A better understanding of user motivation needs to be developed and concerns addressed. If users don't employ them, then the ability to deter theft will be limited.

3.1.3 Organized Fraud/Theft of New Phones

Organized criminals may engage in the collection of large numbers of phones for resale through a variety of mechanisms: purchase of phones under fraudulent contracts, theft of phones from stores/warehouses, etc. Since the phones are acquired at the point of sale, no theft activation mechanisms are likely to be activated at the present. In addition, due to the fact that the fraud/theft operation takes on aspects of a business, the criminals may have more sophisticated attack methods for example, changing the device identifier (e.g., IMEI/MEID)[5]. Phones may be packaged for shipment and use overseas.

3.1.4 Consumer Fraud

Some phones may be misappropriated by fraud. An individual consumer may report the loss of their own phone for insurance collection and attempt to resell their 'lost' phone. It should be expected that the consumer will deactivate any anti-theft mechanisms and revert the phone to its factory state before attempting to resell. Jail-breaking or rooting[6] of the phone may be attempted by the consumer. Anti-theft mechanisms such as a network based blocking approach will be needed to address this form of theft.

3.1.5 Mobile Device Flow Post-Theft

3.1.5.1 Device Discarded

Very common if theft prevention mechanisms are active or the device identifier was blocked by the carrier and the device was not the object of the theft but a side effect: charity bins are a popular route.

Note: Existing solutions and FCC requirements are such that even bricked devices can call "911".

3.1.5.2 Consumer Response

There are a wide variety of possible consumer responses to device theft. First, the consumer needs to recognize the theft has occurred. In some instances, the device theft is witnessed by the consumer. In other instances, the theft may occur without the consumer immediately knowing. For example, the United Kingdom Home Office said… Consumers that know their device has been taken may respond to theft in a variety of ways although many are likely to want to have

[5] For GSM, UMTS, and LTE devices, the GSMA has produced "Security Principles Related to Handset Theft", http://www.gsma.com/publicpolicy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf.

[6] Jail-breaking or rooting of a phone are terms used to describe reprogramming of a phone either to remove restrictions imposed on the phone by a service provider or manufacturer, e.g., limiting phone use to a single carrier or blocking addition of certain applications.

their subscription (SIM card) cancelled to avoid liability for unauthorized voice calls or data traffic. If reported, the consumer may report to a single entity or multiple entities. Consumers may choose to notify law enforcement, insurers, and/or service providers in any combination. For example, having notified law enforcement of a stolen device, a consumer may seek a replacement device from their service provider. Reports of theft to law enforcement may not result in notification to service providers. Dissemination of theft information across all parties affected may be challenging and such direct reporting may need to be supplemented by other mechanisms.

3.1.5.3 Sold Direct to Other Consumers via Auction or Classified Listings Sites

The consumer 'theft awareness and response interval' can vary greatly. Consumers may immediately recognize that a theft has occurred and effectively report the loss to appropriate stakeholders. Alternatively, the consumer may not report the theft to a stakeholder involved in preventing misuse of the phone or may not recognize that a theft has occurred for some time. Thus the sale of a phone to another consumer can occur before a report is lodged or cross network blocking becomes effective. If theft deterrent mechanisms are enabled on the stolen phone at the time of theft, then even without being triggered by the victim and assuming the pin code has not been compromised, this type of disposal is mitigated. As with the theft process described above though, for a stolen device NOT reported because of consumer deceit, device based solutions are intentionally disabled and other fraud prevention mechanisms may be required.

Features that preclude reactivation of a device also mitigate this type of "disposal." Thieves will typically attempt to format a device to restore it to its factory settings. When they do so they will be required to enter a username and passcode that they will not have. This will be an obvious warning sign to a potential buyer. If they do not attempt to reformat and someone attempts to buy the stolen smartphone, the buyer will not be able to reactivate the device. (Hopefully, buyers of used phones through "Craigslist" or other online entities will have some common sense and will make sure the phone functions properly before making the purchase).

3.1.5.4 Sold to Recycling Company

Mobile device recycling is a very competitive market and as a result web based offers try to out-compete each other resulting in good prices being offered and fast turnaround. Companies engaged in this business (including carrier and retailer trade-in and buyback programs) should be compelled, preferably by a voluntary code of conduct rather than regulation, to check the identities of every device they handle against a comprehensive stolen device database. Even with this in place it is acknowledged that the opportunity may exist for a trade to be completed before any 'negative' records about the device come to light. These sales could potentially be mitigated by anti-theft type solutions. No-one accepting used smartphones wants to accept a compromised device; there are simple commercial drivers to avoid this above and beyond the reputational risk.

3.1.5.5 Used in Trade for New Device

Plenty of operators and retailers accept old devices as trade-ins against new devices or contracts, and this presents an opportunity to exchange a stolen phone for a clean phone unless those handling the trade-in devices perform checks against a stolen device blacklist. This is even faster and simpler than the web recycling model and presents an attractive route for the criminal to increase the value of the device even though it may require a little investment. Trade-ins of stolen phone can potentially be mitigated by anti-theft type solutions. The value of a phone that is traded-in with a solution enabled is drastically reduced.

3.1.5.6 Exchanged Under Warranty

Some organizations offer flexible warranty programs with exchanges for phones under warranty being offered easily and quickly. Such schemes leave an opportunity for the exchange of stolen phones for new 'clean' phones, thus successfully laundering the phone and obtaining one to sell that is extremely valuable. Consequently, organizations involved in warranty programs should thoroughly check and record the identities of those exchanging devices and perform device identifier checks against stolen device blacklists on every device presented.

3.1.5.7 Used as Non-cellular Device

It is recognized that stolen devices that may not have been protected with an anti-theft mechanism have a residual value if they can continue to download and execute mobile apps and avail themselves of software updates.

3.2 Mobile Device Theft Statistics

3.2.1 Consumer Statistics

Available data from Consumer Reports (see Section 3.2.2.6) indicate that 34% of consumers fail to activate security mechanisms on their mobile devices. There are likely a variety of reasons for this: mechanisms may hinder use of the device, consumers may not understand the value of the capability or its linkage to theft prevention, activation of the feature may be too easily skipped, etc. Regardless of the specific reasons for consumers not availing themselves of such capabilities, the success of any theft deterrence/mitigation program is dependent upon the broad implementation of these capabilities. To the extent that consumer support is a critical part of this, then theft deterrent programs must have a high rate of consumer acceptance.

3.2.2 Criminal Statistics

There are no current official national law enforcement statistics regarding smartphone theft. The large number of law enforcement agencies in this country (approximately 18,000 according to the results of the Census of State and Local Law Enforcement Agencies conducted by the Bureau of Justice Statistics) makes the aggregation of data from law enforcement agencies a challenge. For the purposes of establishing benchmark figures for tracking purposes, it is recommended that this effort be coordinated with those entities such as cellphone insurance companies, resellers and service providers that may collect pertinent data on an aggregated basis. With their cooperation, deriving theft statistics from their data sets may provide adequate tracking data. This can be supplemented and validated with data from those law enforcement jurisdictions attempting to track this problem. Such case specific information would also be useful for developing better profiles of the different modes of criminal activities.

While no specific nationwide data is available for smartphone theft there are multiple datasets regarding crime.

- FBI crime reporting indicates that theft and robberies in 2012 composed 2972.6 crimes per 100,000 inhabitants.
- Summary data collected by the MDTP Working Group for 21 police jurisdictions indicate that there were 72,772 thefts in jurisdictions covering a population of 19.7 million

residents resulting in a theft rate of 368.9 thefts per 100,000 inhabitants in 2013. Data collected from 8 police jurisdictions covering a population of 7.6 million residents (2013) indicated that theft rate increased by 14.9% between 2012 and 2013.

- Consumer reports in a 2012 survey indicated 1.3 million smartphone thefts and a 2013 survey indicated 3.1 million smartphone thefts. This data would estimate smartphone theft rate of 414 and 981, per 100,000 inhabitants, for 2012 and 2013 respectively. The theft rate increase estimated by this survey is 121.7%.

Collected law enforcement data combined with FBI crime data would estimate that for 2013 one tenth of all thefts and robberies committed in the US is associated with the theft of a mobile device.

Law enforcement data indicates that smartphone based anti-theft solutions deployed in the United States appears to validate the solution as an effective tool to deter smartphone crime.

To truly understand the issue of smartphone crime, accurate data must be provided. There is a significant difference (~2.7x) in crime level reported in the Consumer Reports survey as compared to that reported by a sample of 21 law enforcement agencies. The reasons for this discrepancy need to be resolved. Crime data should also be collected to substantiate the questions of who is stealing the phones and how and where the phones are finding their way back into the ecosystem.

3.2.2.1 Make-up of Criminals (single individuals / organized groups)

Due to the current difficulty in assembling comprehensive information, information obtainable will be largely anecdotal and/or derived from sources with limited geographic scope (e.g., a report from a specific city). In addition, since material from active investigations and prosecutions is kept confidential, there will be a delay in some detailed and relevant information becoming public. With the foregoing, current assumptions are that the majority of crimes at present are relatively unsophisticated “snatch and grabs” with phones reentering the domestic population. More sophisticated crime rings, however are known to exist and some portion of phones are shipped overseas. While current crime trends may suggest early opportunities for mitigation methods that are easily at hand, criminals are adaptive and more hardened solutions should be considered for inclusion over time.

3.2.2.2 Technological Sophistication of Criminal Organization

Comprehensive information is not available. To the extent that a theft mitigation technique is broadly deployed it can be expected that attempts will be made to hack it. Successful hacks will be broadly distributed across the Internet. Those engaged in larger criminal enterprises will have a higher incentive both to develop the necessary skills to re-enable devices as well as make any investments required to acquire any necessary tools.

3.2.2.3 Individual Law Enforcement Data

Policing in the United States is highly-decentralized and primarily a function of state and local government. At last official count 17,985 state and local agencies existed. These included local police agencies, sheriff departments, constable office, state police agencies and special districts such as university police agencies. All combined, these agencies employed 765,246 full-time police officers (Bureau of Justice Statistics, 2011). As can be expected reporting of crimes and data gathering methods vary greatly.

In 1930, Congress authorized the Federal Bureau of Investigation to gather and distribute crime records so as to have a national uniform set of crime statistics. Today, this system known as the Uniform Crime Reporting (UCR) System still exists, but throughout the years it has been met with challenges and limitations. Setting of universal definitions and crime categories has been difficult as state and local laws vary. Although reporting has been good, it is voluntary and agencies may chose not to submit data. More importantly to the effort at hand, there are limited categories in the UCR. Crime categories that are reported include: murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson. Cell phones are the devices taken in one or more of the crime categories and they are not classified as a separate category in the UCR. As no national police data is available, this committee contacted police agencies across the United States in order to gather data. It should be understood that crime reporting capabilities vary greatly among agencies. Agencies are sometimes limited by the ability and sophistication (or lack thereof) of their Records Management System (RMS). For example, in gathering data on cell phones some agencies have to perform key word search and RMS capabilities may have limitations. Additionally, searches may result in underreporting. For example a search for only "iPhones" will not capture crime reports that have "i-phone" or some other spelling variation. All said, the below data is a start as we work toward further understanding this problem.

The data represents a 2013 population base of over 19.7 million or 6.24% of the US population.[7] Based on this data the phone theft rate for 2013 is estimated to be 368.9 per 100,000 individuals. This is significantly lower than the Consumer Reports estimates of the US phone theft rate for 2013 of 981 per 100,000 individuals. The MDTP Working Group was not able to confirm why phone thefts reported to law enforcement is much less than that reported by Consumer Reports.

On a year-over-year basis, the MDTP Working Group observed that the theft rate is increasing but various sources of information show a significant difference level of increase. Data collected from individual police jurisdictions that covered a population of over 7.6 million individuals indicated the rate of theft between 2012 and 2013 increased by 14.9%. Data reported by Consumer Reports indicated the rate of theft between 2012 and 2013 increased by 121.7%.

The MDTP Working Group was not able to confirm why phone thefts reported to law enforcement is much less than that estimated by Consumer Reports.

The data provided from the law enforcement agencies indicate that devices are most frequently taken during crimes associated with Theft/Larceny and 2nd most frequently from crimes associated with Burglary/Robbery.

Data provided for Canada in Section 3.2.2.7.2 indicates that for 2013 the phone theft rate was slightly lower than of the US at 340.3 thefts per 100,000 individuals. Canada data indicated that phones are lost 3.8 times more frequently than they are stolen.

3.2.2.4 FBI Data

The FBI collects data as part of the uniform crime reporting program. To get an estimate of the total theft rate, the subgroup looked at data for both violent crimes where theft and robberies were committed and to property crime statistics. Smartphone theft rate will be a subset of the total theft rate.

[7] Jan 2013 of 316,128,839 estimate from http://www.census.gov/popest/.

Violent crime data indicates that in 2012 there were 354,622 violent crimes with theft and robberies. Property crime data indicates there were 2,103,787 Burglaries and 6,150,598 Larceny-thefts.

The total theft for smartphone will be less than 5,322,344 crimes reported. The total theft rate is 2,859.2 per 100,000 inhabitants for property crime and 113.4 per 100,000 for violent crimes. The total theft rate is 2972.6 per 100,000 inhabitants.

3.2.2.4.1 Violent Crime

In the FBI's Uniform Crime Reporting (UCR) Program, violent crime is composed of four offenses: murder and non-negligent manslaughter, forcible rape, robbery, and aggravated assault.[8] Violent crimes are defined in the UCR Program as those offenses which involve force or threat of force.

- In 2012, an estimated 1,214,462 violent crimes occurred nationwide.
- FBI crime reporting indicates that theft and robberies in 2012 composed 354,622 robberies during violent crimes.

Smartphone theft will be a subset of the theft and robberies committed during violent crimes.

3.2.2.4.2 Property Crime

In the FBI's Uniform Crime Reporting (UCR) Program, property crime includes the offenses of burglary, larceny-theft, motor vehicle theft, and arson. The object of the theft-type offenses is the taking of money or property, but there is no force or threat of force against the victims.[9]

- In 2012 there were 2,103,787 Burglaries and 6,150,598 Larceny-thefts. Of the Larceny-thefts 2,863,935 were of value greater than $200 (Smartphone values are in excess of $200).
- In 2012, the rate of property crime was estimated at 2,859.2 per 100,000 inhabitants.
- Of all property crimes in 2012, larceny-theft accounted for 68.5 percent. Burglary accounted for 23.4 percent and motor vehicle theft for 8.0 percent.
- Property crimes in 2012 resulted in losses estimated at $15.5 billion.

3.2.2.5 Secure Our Smartphone Crime Reports

The Secure Our Smartphones Initiative[10] issued a report which provides crime data for major cities in the US and London.[11] Preliminary statistics following Apple's implementing Activation Lock as part of Find My iPhone appears to validate the solution as an effective tool to deter smartphone crime.

3.2.2.5.1 New York City, New York

Smartphone thefts represent an increasing share of all thefts in New York City. Between 2010 and 2013, the percentage of larcenies from a person involving a smartphone increased from 47

[8] http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/violent-crime/violent-crime.

[9] http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/property-crime/property-crime.

[10] New York State Attorney General Eric Schneiderman and San Francisco District Attorney George Gascón launched the Secure Our Smartphones ("SOS") Initiative in response to the epidemic of smartphone theft and related violence. See http://www.ag.ny.gov/feature/secure-our-smartphones-sos.

[11] Secure our Smartphones Initiative: One Year Later. See http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf.

percent to 55 percent, and the percentage of robberies involving a smartphone increased from 40 percent to 46 percent. In 2013, more than one-quarter of all thefts and over half of grand larcenies from a person (55%) involved a smartphone. Between 2010 and 2013, robberies not involving a smartphone fell by 12 percent, while the percentage involving smartphone grew by nearly the same amount (13%).

New York City also provides evidence that mobile device theft prevention technologies work, as described by the Secure Our Smartphones Initiative in the "One Year Later" report, " In the first five months of 2014, just after Apple introduced Activation Lock, robberies and grand larcenies from a person involving Apple products dropped, respectively, by 19 percent and 29 percent, compared to the same time period in the previous year."[12]

3.2.2.5.2 San Francisco, California

Smartphone theft is responsible for the increasing number of robberies in San Francisco. The majority (59%) of the approximately 4,000 robberies in the City of San Francisco in 2013 involved the theft of a smartphone. The victims of those robberies ultimately recovered less than one in ten stolen smartphones. Apple smartphones constituted the vast majority (69%) of smartphones stolen in San Francisco robberies.[13]

For San Francisco there were approximately 2,360 smartphone robberies (4,000 * 59%) for a population of 837,000, this would result in a smartphone theft rate 282 per 100,000 inhabitants.

Similar to New York City, San Francisco also provides evidence that mobile device theft prevention technologies work. In 2009, Apple smartphones constituted the vast majority (69%) of smartphones stolen in San Francisco robberies; in the six months after Apple made Activation Lock available, iPhone robberies in San Francisco declined 38%.[14]

3.2.2.5.3 London, United Kingdom

Smartphones are a significant driver of thefts in London. Smartphone thefts from a person more than doubled between 2010 and 2013, increasing from 16,141 stolen smartphones in 2010 to 32,872 in 2013. In 2013, nearly half (49%) of London robberies involved a smartphone. Despite a successful 2012 crackdown on smartphone theft, London police still received over 100,000 reports of stolen smartphones in 2013.

London also provides data that mobile device theft prevention technologies work. Thefts of iPhones decreased 24% in the six months following Apple's making Activation Lock available.[15]

3.2.2.6 Other Studies on Mobile Device Theft

Consumer Reports estimates that 1.6 million Americans had their smartphones stolen in 2012. By 2013, they reported 3.1 million victims, a 94% increase in just one year.[16] Consumer report also provided data regarding how smart-phone users secure their phone:

[12] Secure our Smartphones Initiative: One Year Later. See http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf.

[13] The relative percentage of robberies involving devices from particular manufacturers is expected to shift as anti-theft, like Apple's Activation Lock, become more widely available.

[14] Secure our Smartphones Initiative: One Year Later. See http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf.

[15] Secure our Smartphones Initiative: One Year Later. See http://www.ag.ny.gov/pdfs/SOS%201%20YEAR%20REPORT.pdf.

[16] http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

- Set a screen lock with a 4-digit pin (36 percent).
- Backed up data to a computer or online (29 percent).
- Installed software that can locate the phone (22 percent).
- Installed an antivirus app (14 percent).
- Used a PIN longer than 4 digits, a password, or unlock pattern (11 percent).
- Installed software that can erase the contents of the smart phone (8 percent).
- Used security features other than screen lock (e.g., encryption) (7 percent).
- Took none of these security measures (34 percent).

This data is based on the Consumer Reports National Research Center annual State of the Net survey conducted in January, 2014. The findings are nationally representative of U.S. adult Internet users. Participants were 3,110 adults with a home Internet connection who were part of an online panel convened by GfK. From those respondents, Consumer Reports made national projections. The margin of error for the full sample was ± 1.8 percent, and ± 2.4 percent for the subset of Internet-connected smart phone owners, both at a 95 percent confidence level.[17]

3.2.2.7 Data from Carrier Initiatives

The number of devices added to the GSMA's IMEI Database is readily available. This includes devices added to the blacklist and removed from the blacklist.

In compiling and providing these figures a few matters came to light as follows:

- It is clear from the operator by operator breakdown that there are differences between the operators in terms of what, when and why they block devices. GSMA, through the North American Regional Interest Group, will facilitate discussions between the operators to establish consensus in terms of blacklisting policies going forward to ensure consistency of what is blocked and measured.
- The figures provided represent the monthly net difference between what was blacklisted and un-blacklisted. Therefore, a greater number of devices were blacklisted each month but a significant number were subsequently un-blacklisted, presumably because a proportion of the devices originally blacklisted were recovered.
- The figures include not only stolen devices but also lost devices as these are also blocked by some, if not all, operators. Consequently, the total figure for the year is not exclusively a theft figure as lost devices are included.
- The trend shows an increase in blacklisting levels over the 12 months but it would be too simplistic to equate this to an increase in loss or theft levels. In other countries where similar initiatives have been taken to combat handset theft the data also shows initial increases in the blacklisting rates. This can be attributable to the fact that consumers are more likely to report their devices lost/stolen as awareness of the blacklisting capability increases and also that operators, often after a tentative start, are more inclined to block devices as they become comfortable with the concept and their processes over time. None-the-less, the data clearly does indicates that the number of "lost and stolen" devices is at the millions per year level.

Although it is possible to extract figures based on the number of blacklist records on the GSMA IMEI Database, as has been done, it is not clear how representative they may be of the actual

[17] http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html.

handset theft levels in the US due to anomalies that may currently exist. That said, GSMA and the service providers understand the duty industry has to compile figures that could be useful to ascertain theft levels. To that end GSMA has committed to work with the service providers in the near future with a view to agreeing guidelines on what to measure and report on going forward. Knowing clearly that we are still in the relatively early stages of the roll-out is very promising suggesting a much greater impact of the use of the database going forward.

3.2.2.7.1 United States

The following data includes the four major national carriers; it is important to note that the U.S. is still in start-up mode in using the database so some of the increase is clearly attributable to this fact. The data includes both lost and stolen phones.

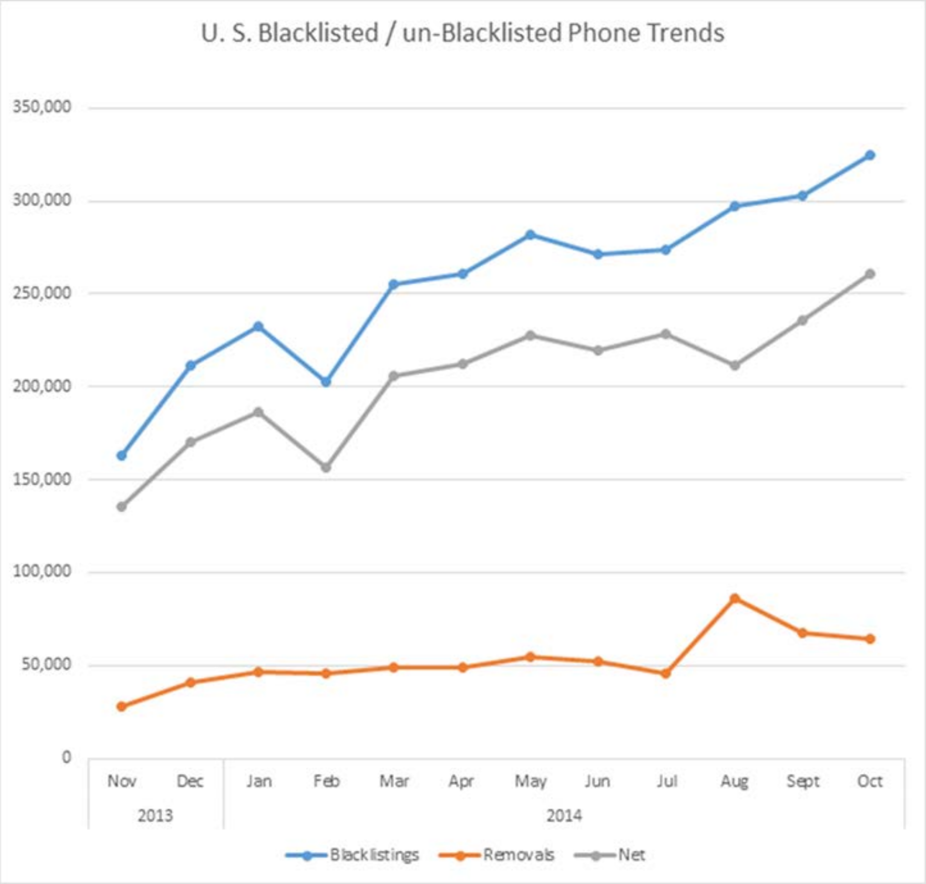


Figure 4: US Blacklisted / un-Blacklisted Phone Trends

3.2.2.7.2 Canada

The Canadian Wireless Telecommunications Association (CWTA) is the recognized authority on wireless issues, developments and trends in Canada. It represents wireless service providers as well as companies that develop and produce products and services for the industry, including handset and equipment manufacturers, content and application creators and business-to-business service providers.

CWTA and its members have always taken the security of all aspects of the Canadian wireless system very seriously. The wireless industry has made significant commitments and investments to reduce incidences and the impact of mobile device theft in Canada, including: a national educational campaign; the "Protect Your Data. Protect Yourself" initiative and Web site; the national blacklist for lost and stolen devices; and the public IMEI lookup tool, which was used by Canadians more than 400,000 times over the past year to check the status of a pre-owned device.

CWTA has also facilitated direct-access connections to the GSMA IMEI Database for nine Canadian law enforcement agencies, including national, provincial and regional forces. Currently, five additional LEAs are in the process of applying for access to the Database. GSMA confirms that Canada has more LEAs with direct connections to the IMEI Database than any other country in the world.

As part of CWTA's ongoing commitment to monitor and combat wireless device theft, CWTA provides the Canadian Radio-television and Telecommunications Commission updated statistics on devices reported lost or stolen on a periodic basis.

In the following data:

1. Figures are reported by province based on the area code of the phone number associated with the device reported as lost or stolen.
2. Not all service providers record lost and stolen devices separately. Those that do record lost and stolen devices separately do so based on the customer's report only. The industry-wide breakouts provided below are based on applying the provincial percentages of phones reported lost or stolen to the total lost/stolen numbers provided by those who do not distinguish between the two. Because of the scope of the service providers that do differentiate between lost and stolen devices based on customer reports, the numbers below should be considered statistically significant.
3. The variation in the year-to-year figures presented below is partly attributable to a lack of standardized recording and reporting practices that existed before CWTA initiated industry-wide handset security measures – including the public reporting commitment – in November 2012.

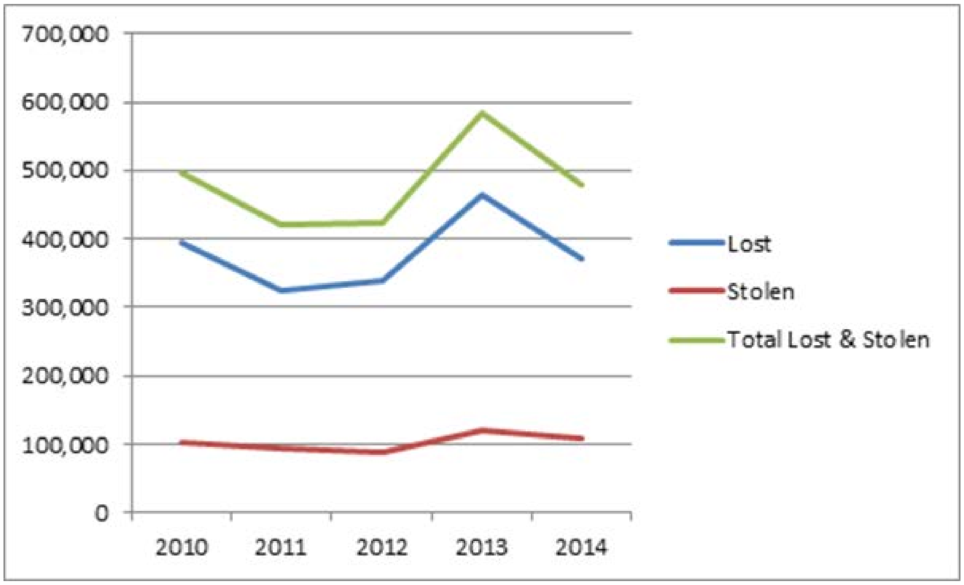


Figure 5: Canada Lost & Stolen Phones by Year

Table 3: Canada Lost & Stolen Phones by Province by Year

Region/Province		2014*	2013	2012	2011	2010
British Columbia	Lost	49,710	64,717	53,516	51,281	60,980
	Stolen	17,025	18,161	13,090	14,007	16,931
	Total Lost & Stolen	66,735	82,878	66,606	65,288	77,911
Alberta	Lost	46,013	63,821	51,201	48,512	54,856
	Stolen	13,142	14,867	11,890	12,008	14,308
	Total Lost & Stolen	59,155	78,688	63,091	60,520	69,164
Saskatchewan	Lost	14,877	15,265			
	Stolen	4,384	4,277			
	Total Lost & Stolen	19,261	19,542			
Manitoba	Lost	11,918	16,198			
	Stolen	3,601	4,024			
	Total Lost & Stolen	15,519	20,221			
Saskatchewan/ Manitoba	Lost			21,593	18,779	17,351
	Stolen			5,837	5,756	4,832
	Total Lost & Stolen			27,430	24,535	22,183
Ontario	Lost	170,446	206,215	153,422	148,453	171,674
	Stolen	48,326	54,016	40,366	43,201	46,773

Region/Province		2014*	2013	2012	2011	2010
	Total Lost & Stolen	218,772	260,231	193,788	191,654	218,447
Quebec	Lost	63,078	75,093	42,655	57,206	70,555
	Stolen	18,168	18,137	11,396	15,368	14,359
	Total Lost & Stolen	81,246	93,230	54,051	72,574	84,914
New Brunswick	Lost	1,335	6,389			
	Stolen	4,513	1,559			
	Total Lost & Stolen	5,848	7,949			
Nova Scotia	Lost	5,778	9,569			
	Stolen	1,647	2,343			
	Total Lost & Stolen	7,426	11,913			
Prince Edward Island	Lost	709	1,272			
	Stolen	206	320			
	Total Lost & Stolen	915	1,592			
Newfoundland and Labrador	Lost	3,025	5,140			
	Stolen	903	1,426			
	Total Lost & Stolen	3,928	6,566			
Atlantic Canada	Lost			14,802	13,973	18,558
	Stolen			3,704	4,201	5,084
	Total Lost & Stolen			18,506	18,174	23,642
North	Lost	1,206	2,013	529		
	Stolen	358	512	133		
	Total Lost & Stolen	1,564	2,525	662		
Canada	**Lost**	**371,273**	**465,693**	**337,718**	**325,626**	**393,978**
	Stolen	**109,096**	**119,642**	**86,416**	**94,542**	**102,288**
	Total Lost & Stolen	**480,369**	**585,336**	**424,134**	**420,167**	**496,266**

* indicates data is year to date totals as of September 2014.

Table 4: 2013 Phone Theft Rate for Canada[18]

Region / Province	Thefts	Population (x1,000)	Theft Rate (Per 100,000)

[18] Canada Population estimates for 2013 http://www.statcan.gc.ca/pub/91-520-x/2014001/tbl/tbl3.1-eng.htm.

Region / Province	Thefts	Population (x1,000)	Theft Rate (Per 100,000)
British Columbia	18,161	4,582.00	396.4
Alberta	14,867	4,025.10	369.4
Saskatchewan	4,277	1,108.30	385.9
Manitoba	4,024	1265	318.1
Ontario	54,016	13,538.00	399.0
Quebec	18,137	8,155.30	222.4
New Brunswick	1,559	756.1	206.2
Nova Scotia	2,343	940.8	249.0
Prince Edward Island	320	145.2	220.4
Newfoundland and Labrador	1,426	526.7	270.7
North (Yukon, Northwest Territories, Nunavut)	512	115.8	442.1
Canada Total	**119,642**	**35,158.30**	**340.3**

3.2.2.8 Data from Third-Party Database Providers

In a Latin America pilot, the iconectiv Device Registry aggregated the national blacklist and approximately 1 billion Call Detail Records (CDRs) from Mobile Network Operators (MNOs) in the country with over 12 million subscribers. Key findings included:

1. The percentage of stolen devices was 7.24%.
2. Trend analysis showed that the top 10 devices on the Blacklist comprised largely of Samsung and Nokia smartphone models. This was different from the top 10 devices in the country which also included Apple and Blackberry devices.
3. It was noticed that certain IMEIs keep appearing and disappearing from the national blacklist. Deeper analysis revealed that for a single suspicious IMEI, there were 80,000 cloned devices in the country –a key problem for service providers as it would mean that network blocking would shut off 80,000 customers! This demonstrated a key gap in simply blocking devices without attesting the validity of the identifier.

3.3 Mobile Device Information

It may be useful as part of the device activation process to acquire information from the phone that could be used for theft prevention/mitigation purposes. Some consideration should be given to whether such information is currently collected and how is it utilized. There may be privacy and security concerns associated with the collection of such information that should also be part of the discussion. In this regard, an analogy was to Operation Safe Kids where child fingerprint information is retained by the parent and not the law enforcement agency. Privacy concerns, if such exist, could be mitigated if access to such data was restricted to the consumer, perhaps via their device's cloud account.

3.4 *Industry Policies*

Some industry groups (e.g., CTIA and GSMA) have developed policies on theft mitigation that can be adopted by individual members. However, not all relevant stakeholder groups have such policies in place. Meaningful theft policies should be in place among all such groups to educate stakeholders, to better identify pragmatic steps that should be taken as well as to incentivize implementation of effective measures.

The GSM Association's North American Fraud Forum and Security Group (NAFFSG) developed and published in May, 2012 an "Analysis and Recommendations for Stolen Mobile Device Issue in the United States". The conclusions and recommendations by the NAFFSG can be summarized as follows:

1. Implementations and procedures within an operator network are wireless operator specific.
2. It is recommended that GSMA North American Regional Interest Group wireless operators share blacklisted (e.g., stolen) mobile device IMEIs.
3. IMEI sharing and coordination is recommended to be via the GSMA IMEI Database.
4. The recommended solution, while broad in nature, is not a global solution as not every mobile network operator in every country is connected.
5. IMEI tampering negatively impacts the effectiveness of blacklisting.
6. Blacklisting provides no prevention of using a stolen device to obtain WiFi only services, nor will the recommendations address WiFi-only mobile devices.
7. The current threat profile may change in future as criminals learn new techniques to defeat wireless operator security mechanisms.
8. Barring of stolen devices on its own is insufficient to fully address the problem of device theft.

3.5 *Laws – State and Federal*

3.5.1 Existing Laws

3.5.1.1 Smartphone Anti-Theft Legislation

Minnesota's[19] recently passed a law[20], closely followed by California[21] requiring smartphones sold in those states to have anti-theft functionality to be enabled by default. (See Appendix B Minnesota law and Appendix C for California law.)

The result of the CTIA voluntary commitment[22] along with the laws in place for Minnesota and California is that anti-theft solutions on smartphones will be deployed across the device ecosystem.

[19] http://www.house.leg.state.mn.us/bills/billnum.asp?billnumber=SF1740.

[20] See Appendix 1 – Minnesota State Law.

[21] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB962. See Appendix 2 – California State Law.

[22] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

3.5.1.2 Second-Hand and Pawn Licensing Requirements

Second-hand compliance does not exist in all jurisdictions. Pawn license compliance exists in more jurisdictions.

The United States has some of the most diverse second-hand trade laws in the world. Requirements and enforcement vary greatly, with States, cities and municipalities having different, sometimes conflicting requirements. Some states have no requirements; others go so far as to require thumbprints, photographs or copies of State I.D.s to be recorded. Typically, whatever records are required must be made available to the local Police Department (PD) responsible for enforcing licensing requirements.

These records are created AFTER a transaction takes place. So typically, a pawn or second-hand transaction will occur, the seller's details and the transaction data will be stored according to local licensing requirements and then transmitted by an agreed method to the local PD.

3.5.2 Planned Laws

Many other states are in the process of considering legislation (see Table 5) and any differences, even minor, could result in the requirement that a different model of a smartphone be manufactured for sale into that state for compliance with the local laws.

Table 5: Planned State Laws

Bill	State	Last Action Date
HB 2112	Puerto Rico	9/11/2014
SB 1060	Michigan	9/16/2014
H 1281	Virginia	8/28/2014
A 3157	New Jersey	5/15/2014
H 8115	Rhode Island	5/6/2014
S 2897	Rhode Island	4/10/2014
A 8984	New York	5/30/2014
S 6850	New York	3/19/2014
SB 3539	Illinois	4/11/2014
TBD	New Mexico[23]	TBD
TBD	Nevada	TBD

[23] Proposed legislation to be discussed at 19 November 2014 meeting of the Science, Technology and Telecommunications Committee, http://www.nmlegis.gov/lcs/agendas/sttcagenov18.14.pdf.

Draft Federal Legislation has also been introduced.

Table 6: Planned Federal Laws

Bill	Author	Last Action Date
S. 2032	Klobuchar, D-MN	2/12/2014
H.R. 4065	Serrano, D-NY	2/21/2014

Due to the various statuses of bills passing through their respective processes, most of the requirements and provisions in draft legislation are not consistent among the proposed draft bills or currently enacted state laws. If the bills remain unchanged and progress to passage, the laws may result in significantly different requirements for devices between states and could require devices to be manufactured uniquely for each state. There is a risk that this would increase consumer cost for devices and reduce their choice of smartphones selection.

3.6 Device Owner Reaction to Mobile Device Theft

Device owner reaction to a theft will vary. In a robbery, the prime concern of the victim is for their safety. Beyond personal safety, it may be that the next concern of the consumer is for replacement or recovery of the device, with the loss of data a secondary concern. However, the increasing use of devices as repositories for all types of personal information, their easy access to information online and their increasing use as payment devices suggests that safety of data resident on a phone needs to be an increasing consideration if not becoming the primary consideration. If a person's identity can be extracted from the smartphone, the criminal with that information can easily acquire additional smartphones, among other things, as has been demonstrated in the case of the "Mustafa Organization" in Minneapolis in August 2014.[24]

3.7 Other Stakeholder Response to Mobile Device Theft

3.7.1 Carrier/Providers

Each mobile device contains a unique identifier that allows individual devices to be permitted or denied network access through the use of network registers. As devices attempt to obtain service on mobile networks their identifiers are transmitted to the networks and are checked against a blacklist of stolen devices.

The efficient blocking of stolen devices on individual networks depends on the secure implementation of the device identifiers on all mobile handsets. The world's leading device manufacturers agreed to support a range of measures to strengthen IMEI security to provide confidence in device blocking and the deployment of enabling technologies and progress is monitored by the GSMA.

The four largest US carriers have invested in the network infrastructure necessary to block devices on their networks and they act on reports of device loss/theft from their customers by placing the device identities on a blacklist, which ensures that the devices are blocked on the home network. Moreover, because the carriers share data through the global GSMA IMEI

[24] http://www.startribune.com/local/minneapolis/270960821.html.

Database, the blocking of a device on one network becomes effective on the other technology specific networks.

3.7.1.1 Cross Network Blocking (GSMA)

The industry recognizes the need to ensure that stolen mobile devices can be rendered useless in order to reduce their value on the black market, removing all incentive for thieves. The GSMA has led a number of initiatives to combat mobile device theft and it strongly encourages network operators to deny connectivity to any stolen device. Furthermore, GSMA invites networks to connect their individual databases to the GSMA's IMEI Database to ensure devices stolen from their customers can be blocked on every other network around the world that also uses the IMEI Database. The IMEI Database solution is available to operators to use free of charge and all mobile carriers are encouraged to submit and share stolen device data. The Database has been in place for many years and device blocking and data sharing has had a positive impact of mobile device theft levels in many countries.

A truly effective campaign against device theft must be multi-faceted and a range of measures must be put in place that complement each other. The emergence of the device based anti-theft measures concept is an interesting development that is entirely complementary to, as opposed to an alternative to, network blocking.

In addition to the IMEI Database supporting stolen device data sharing between operators, GSMA offers a look up service to industry stakeholders and law enforcement agencies to support checking of mobile device identifiers against the registry of lost and stolen devices.

3.7.1.2 Law Enforcement

It does not appear law enforcement has fully utilized the various alerting databases that are available. To be effective, law enforcement must understand the process for getting access to a stolen device database, and the information provided must be made relevant to their work. Information provided should address all types of mobile device theft across all service providers. Integration into other existing national crime databases may be desirable. It should be determined what processes/interfaces would be most relevant to law enforcement for purposes of identifying stolen mobile devices. Current databases have seen little use from the law enforcement community. Many in the community are not aware of their existence and those aware are not convinced of their utility. Given the challenges in addressing the thousands of separate agencies, the intended utility of the databases within the context of the law enforcement agencies' daily functioning should be carefully defined with law enforcement needs in mind.

3.7.2 Insurance

Mobile device theft is a regrettable crime for the consumer from multiple standpoints. Among other considerations are the consumer's safety, economic loss, inconvenience and other hardships. From the standpoint of the insurance administrator, theft is just one of many modes by which consumers can lose the utility of their device and drive the need for a replacement. Other modes include physical damage, water damage, loss, and malfunction. All modes, including theft scenarios in particular, raise the need for consumer education on how to protect the physical phone and data, simple and rapid means for replacing the phone for the consumer, and a means by which phones that are recovered/returned in the supply chain with a lock enabled can be quickly and easily unlocked by the new legal and rightful owner of the phone (e.g., insurance administrator, etc.) so that it may be re-used or re-cycled in the reverse logistics supply chain.

3.7.3 Databases

Discrete databases may serve an important function for service providers, recyclers and insurance companies in their daily operation. However, for most effective use as a deterrent tool for various stakeholders, focus should be a single data source which integrates necessary information from other sources. Characteristics of such a database would include:

- Information in a timely (real-time/immediate) fashion. On average, the time lost from device theft (the instant the thief has the device in hand) to when the device gets into the database is dependent on when the wireless operator is notified of the stolen device by the customer. Once the customer reports the stolen device, the customer's wireless operator may immediately put the stolen device on the blacklist. Included in this time delay factor is the time between when the device is stolen and when the victim recognizes it has been stolen, the time between when victim recognizes the device is stolen and when the victim figures out who to notify and acquires a means of accomplishing the notification since their primary communication device has just been taken, and the administrative delays in uploading the information.
- Information on all mobile device types.
- Information from all service providers.
- Information from all network types.
- Information from service providers, law enforcement, insurers, recyclers; basically all entities that are reporting points for device theft.
- Standardized interfaces and possible support of major reporting systems.
- Coordinated with both law enforcement and legal experts on permitted forms of access and information distribution.
- Coordinated and accurate reporting of stolen devices would be necessary to track progress. Reporting capability should be aligned across geopolitical boundaries to better coordinate with local law enforcement.

3.7.4 Device Manufacturers and Operating System Providers

Existing or planned mobile device theft prevention solutions rely on both of two approaches:

1. Device-based solutions that when triggered (usually over the network) disable device functionality.
2. Network-based solutions that block network access by unique device identifiers that have been reported to central databases as stolen.

In either of these approaches, depending upon implementation, there are varying risks of tampering that could defeat theft prevention mechanisms. Currently, there is one study showing the impact to the overall anti-theft ecosystem since the implementation of Apple's Activation Lock in September of 2013.[25] Long term efforts to increase the trust level of a device, efforts to

[25] The report also revealed new crime statistics showing that, after Apple added a "kill switch," robberies and grand larcenies involving iPhones plummeted. Simultaneously, violent crimes against people carrying phones without a kill switch surged. The data is part of a new report issued by the Secure Our Smartphones ("S.O.S.") Initiative, an international partnership of law-enforcement agencies, elected officials and consumer advocates, which will mark its first year tomorrow.

provide devices with truly immutable data elements would help in identifying stolen mobile devices.

4 Existing Solutions

This section provides high-level representations of existing and pending solutions and solution components from across the globe and identifies capabilities and impacts as they associate to the "aspirational" Consumer Response Flow.

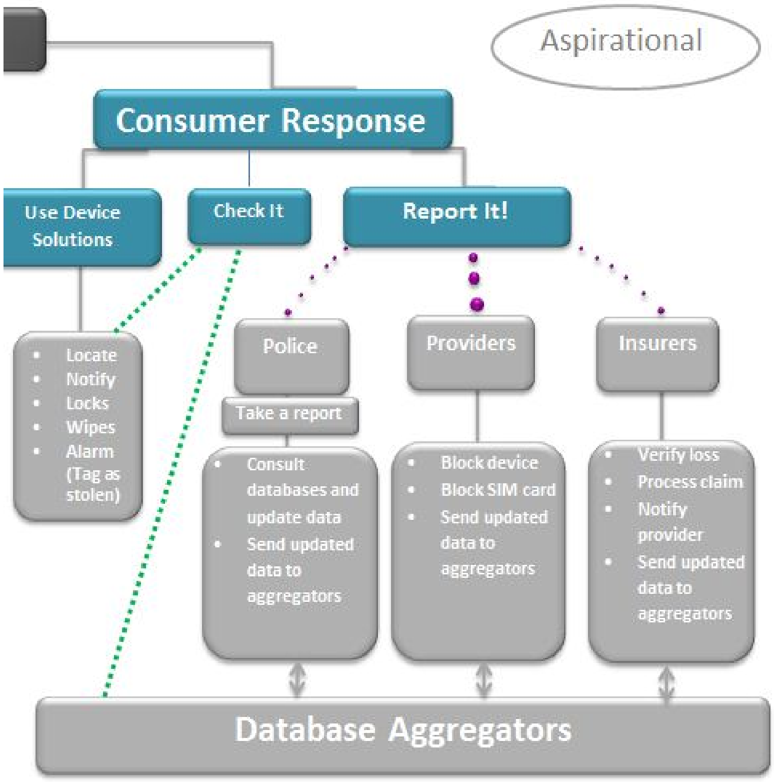


Figure 6: Aspirational Consumer Response Flow

In New York City, theft of iPhones fell significantly after the release of Apple's Activation Lock on September 18, 2013, as indicated in the chart below. In the first five months of 2014, robberies and grand larcenies involving Apple products dropped 19% and 29%, respectively, compared to the same time period from 2013. The decrease in Apple thefts far surpassed the citywide decrease in all robberies (-10%) and all grand larcenies (-18%). Perhaps most tellingly, robberies and grand larcenies from a person involving a Samsung smartphone, which did not have a kill switch during much of this time, increased by over 40%. (Encouragingly, Samsung introduced a kill switch solution in April of 2014 on their Verizon Wireless devices, the impact of which will likely be seen in future statistics.) Statistics from San Francisco and London show similar outcomes. In San Francisco, iPhone robberies declined 38% while robberies of Samsung devices increased by 12%. In London, Apple thefts declined by 24% while Samsung thefts increased by 3%. (In both cities, data from six months leading up to Apple's Activation Lock was compared to the six months following its introduction.) http://sfdistrictattorney.org/index.aspx?page=357.

The following subsections provide summary descriptions of the existing solutions. The detailed information for the existing solutions is provided in Appendix D. The summary descriptions are grouped into the following categories:

- Database Solutions.
- Device Based Solutions.
- Third Party Solutions.
- Wireless Operator Implementations.

4.1 Database Solutions

(A) **Repositories of mobile device information catering to specific services exist including a national/global mobile registry, insurance databases, and law enforcement databases.**

A national/global mobile registry typically comprises IMEI information. Such registries are also used to provide identities for Government e-Services, mobile commerce and national security purposes. A 2013 GSMA report[26] describes the growth of such a registry around the world with 80 countries either having one or thinking of developing one.

Other repositories include the solutions from some manufacturers or in partnership with some manufacturers. Any reversible (by the consumer) locking or disabling feature inevitably requires that a record be made of the devices current status and retained by the solution provider. These databases are proprietary where they exist and current experience suggests they are not shared with aggregators meaning the stolen status they reflect, if not also additionally reported by the consumer to a network or police will be impossible to determine other than by physical inspection.

(B) **Databases of reported stolen devices such as the GSMA IMEI Database**.

The GSMA North American Regional Interest Group (GSMA-NA) "Analysis and Recommendations for Stolen Mobile Device Issue in the United States" recommended that GSMA-NA wireless operators share blacklisted (e.g., stolen) mobile device IMEIs, with IMEI sharing and coordination recommended to be via the GSMA IMEI Database.

The GSMA IMEI Database is a global list that is the primary method used by carriers to enforce the ability to deny service to stolen mobile devices on the operator networks. The IMEI is a standardized 15-digit number that is used to identify the device when it is used on a mobile phone network. The IMEI must be unique for each device, so there needs to be a way of managing allocations of IMEIs to handset manufacturers to ensure that no two devices use the same IMEI. The GSM Association performs this role, and records all of the IMEIs that are allocated to mobile device manufacturers in the GSMA IMEI Database. When reserving IMEIs for a device manufacturer, the GSMA stores some basic information associated with the IMEI. This information includes the manufacturer name and the model identifier of the associated handset and some of its technical capabilities (e.g., frequency bands supported by the handset, the handset power class, etc.). The GSMA IMEI Database also supports what is known as a "black list". The black list is a list of IMEIs that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use.

[26] http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

Network operators who deploy Equipment Identity Registers (EIR) or other Fraud Management Systems in their networks use the black lists to keep their own lists of blacklisted lost or stolen phones. Operators' EIRs automatically connect to the GSMA IMEI Database to share their latest lists of blacklisted devices with other operators. The GSMA IMEI Database takes the black lists from the various operators around the world that are connected to the system and compiles the data into one global black list. When a network operator EIR subsequently connects to the GSMA IMEI Database, it downloads the latest global black list (or a national or regional subset of the global list) for its own use. By loading the GSMA IMEI Database black list onto the local EIR, all handsets reported as stolen on other connected networks up to the previous day are now also capable of being blocked on that network. The GSMA IMEI Database has broad support from 95 GSM & LTE operators in approximately 55 countries. It is dependent on the reporting frequency of mobile device theft and is capable of more frequent updates than some operators currently make use of, which is typically once daily (note – some operators upload their data nearly instantaneously, while the download of data may be daily). The GSMA IMEI Database is searchable by law enforcement agencies and by traders globally though as with other options, awareness and uptake is very low. The GSMA IMEI Database is also capable of taking MEID data from CDMA carriers and is not just restricted to taking IMEI data from GSM/UMTS/LTE carriers.

(C) **Database aggregators that integrate mobile device data from multiple sources including those mentioned above**. **Key examples include: iconectiv Device Registry and Recipero.**

The iconectiv Device Registry is a comprehensive centralized device analytics solution that automatically discovers mobile device data from multiple sources including Operator networks to provide powerful insights regarding mobile devices. By consolidating real-time and non-real time data collection of mobile data in a common context, Device Registry product can address both traditional mobile equipment challenges, such as anti-theft, invalid device blocking and cloning detection, and also provide lifecycle analysis of mobile devices and subscribers over multiple data pivot points—such as IMEI, IMSI, MSISDN—while providing a valuable source of information for manufacturers, Operators, national regulators, customs and taxation, law enforcement and national security organizations. It is not limited to IMEI only devices. It can analyze different device types such as Data-only Wi-Fi devices, wearables, IoT devices and even feature phones. It correlates patterns across aggregated devices and can be used to detect mobile crime as well as provide Business Intelligence. It has a SMS capability to reach subscribers to validate device status.

Recipero operates a suite of products aimed at reducing mobile device crime. Recipero aggregates data from the GSMA system above and adds to this, CDMA loss/theft reports, insurance claims, finance agreements, police crime reports, corporate thefts, supply chain losses, and voluntary ownership registration by the public. Searches against this large dataset are provided to the trade and to law enforcement. The LEA service is oriented to LEA needs in terms of evidence chain and auditing and the trade service is highly optimized for volume traders. The service is global, ensuring that devices not deemed to be in the hands of the rightful owner are prevented from trade wherever the trade checking service is used. Across the US, there are in excess of 11,000 trading points using Recipero's service to avoid buying stolen property. Across the UK and Europe there are another 8,000 trading points. Around 2 million trader and consumer checks are performed each month. The law enforcement tool is provided free of charge and is believed to be the most widely used law enforcement tool globally for tracing stolen property.

4.2 Device Based Solutions

With access to the operating system on the smartphone, device-based solutions go beyond what is possible with operator and database aggregation solutions when it comes to restricting the functionality of a smartphone. As long as there is Internet connectivity, via a cellular network or WiFi, device-based solutions can be remotely operated to impose restrictions or trigger functions to protect data, audibly draw attention, or determine the current location of the smartphone. Some solutions provide a level of protection even when internet connectivity is unavailable.

Representatives from Apple, Blackberry, Microsoft, Motorola Mobility, and Samsung directly provided information about current solutions offered with some or all smartphones sold by those companies. LG provided information on current solution with some smartphones sold by the company and on future LG solutions to fully meet State Laws on kill switch. Qualcomm directly provided information on a future solution that will be offered by the company. Google did not have an official representative, although an outline of their solution was provided. This information is contained in Section D.2 of Appendix D.

Most device-based solutions discussed in this document are provided to consumers free of charge as part of their smartphone purchase, if the smartphone has the technical capability to run the solution (e.g., supported OS version, certain hardware security features, etc. – requirements varies by solution). iOS and Windows Phone OS provide device-based solutions that work on all smartphones running those operating systems and neither exposes APIs for third party device-based solutions; Android provides a device-based solution, but several manufacturers choose to replace or extend that solution using APIs provided by the operating system vendor.

While specific behaviors may vary slightly, all solutions (except Qualcomm) provide these basic features:

- Locate – get current location of the smartphone.
- Ring – ring or make noise even if the speaker is muted to help find smartphone.
- Lock with PIN – prevent access to information and apps on the smartphone.
- Erase – remove user information from the smartphone.
- Web Interface – a portal to remotely trigger and view status of the above actions.

In addition, since September 2013, Apple and Samsung have introduced features that:

- Prevent reset without the user's authentication – making the smartphone useless to non-authorized owners.
- Require user authentication to unlock – generally stronger than a simple PIN.

Some solutions provide data backup and restore as part of the solution while others rely on operating system backup and restore functionality to assist users with data recovery in the event of loss or theft.

Qualcomm's solution differs from the other solutions in that it's more a component that may be used in the future by device-based solutions. It provides an additional layer of protection by exposing a chipset-level hardware lock when a device is disabled. This component will be available for solution providers to consider integrating next calendar year.

Apple, Google, LG, Microsoft, Motorola Mobility, and Samsung have all signed on to the CTIA Smartphone Anti-Theft Voluntary Commitment[27] and will meet the requirements set forth in that document by the July 1, 2015 date. Several of these existing solutions provide much of what is required in the State laws and Voluntary Commitment, with some solutions already meeting the agreed upon functionality. All solution providers are working on revisions to add any additional and/or necessary capabilities.

4.3 Third-Party Solutions

Three third-party solutions have been considered, “Absolute LoJack”, “Lookout”, and “AT&T Mobile Locate”. Absolute LoJack benefits from OEM cooperation, as it is integrated beneath the operating system (OS Layer), ensuring substantial resilience against software resets. Absolute LoJack is available on Samsung Galaxy Mobile Devices and Windows Surface Pro 3. In some respects, given its tight device integration, Absolute LoJack may be considered a device solution, rather than third-party Solution. However, consumers may purchase a less integrated version of Absolute LoJack on their device once the device is initially activated, enjoying only a subset of the more integrated version’s benefits. Absolute LoJack is very focused on the potential recovery of lost or stolen devices, and devotes a substantial investigation team to support this objective.

Lookout offers compatibility with a wide range of devices, although its remote lock and wipe functions are limited to android devices. Its software sits on top of the operating system, so it is potentially removed with reinstallation of the OS. Lookout’s features are oriented toward internal security rather than device recovery in the event of theft. For example, Lookout is surveying for malicious software that may cause problems for the owner. As long as Lookout is active on the (Android) device, Lookout is able to provide location alerts and alerts about key events such as SIM removal or feature disablement that may be indicators of theft activity.

AT&T Mobile Locate is a solution through an application available for both Apple and Android devices for AT&T subscribers.

4.4 Operator Solutions

This section is a summary of information shared by Sprint, AT&T, T-Mobile, and Verizon.

In April, 2012, the major operators agreed to:

1. Implement databases to prevent reactivation of stolen smartphones, and
2. Educate consumers about applications to remotely lock/locate/erase data from smartphones.

The major operators agreed to work to initiate, implement and deploy database solutions, using unique smartphone identifying numbers, designed to prevent smartphones reported by their customers as stolen from being activated and/or provided service on their own networks. This resulted in the GSMA-NA’s “Analysis and Recommendations for Stolen Mobile Device Issue in the United States”. By using unique GSM smartphone identifying numbers (“IMEIs”), GSM providers developed and utilized the GSMA IMEI Database designed to prevent GSM smartphones reported as stolen from being activated or provided service. By October 31, 2012, U.S. GSM implemented connectivity to this database so that stolen GSM smartphones will not work on any U.S. GSM network whose operator supported the voluntary agreement. In addition, U.S. providers are using the GSMA IMEI Database as a common database for LTE smartphones

[27] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

designed to prevent smartphones that are reported stolen by consumers from being activated or provided service on any LTE network in the U.S. and on appropriate international LTE stolen mobile networks. This database was completed by November 30, 2013.

The major operators also informed consumers, using communications including email or text messages, about the existence of – and access to – applications that can lock/locate/erase data from smartphones. Providers will also educate consumers on how to access these applications, including those that are easy-to-find and preloaded onto smartphones. This was completed by April 30, 2013.

All of the major carriers have also signed the CTIA facilitated Smartphone Anti-Theft Agreement[28] and intend to support the various enacted state laws on Kill Switch. Each of the major carriers conduct various consumer outreach activities, supports Law Enforcement partnerships and cooperation, and actively pursues consumer messaging in the realm of theft prevention.

All of the major carriers have similar integration with the GSMA IMEI Database with daily database synchronizing (uploads and downloads) of lost or stolen GSM and/or LTE Device IMEI information (see GSMA-NA's "Analysis and Recommendations for Stolen Mobile Device Issue in the United States"). Additionally, the major carriers maintain their own in-network Equipment Identity Register (EIR) or "blacklist database" that enables the carrier to block service of all blacklisted lost or stolen devices, including blocking provision of said devices in their entirety. Furthermore, Sprint synchronizes lost or stolen CDMA devices with Recipero's database/ecosystem and utilizes Recipero's CheckMEND to avoid purchasing stolen devices in their buyback program.

All of the major carriers offer insurance for certain mobile devices. The insurance typically provides coverage for several perils including phone theft. Customers opt-in and pay a premium typically in the form of a monthly fee. Not all users opt-in for insurance protection from their wireless carrier. Asurion is one of the administrators of insurance programs on behalf of wireless carriers. For example, Asurion is the administrator for the AT&T, Verizon and Sprint programs.

All of the major carriers, in addition to other entities that manage reverse logistics of returned devices, share the concern of receiving devices with no way to first ensure the device is unlocked by the authorized owner, or to unlock (or unprotect) as the new authorized owner. Without such a solution in place, it is anticipated that numerous quantity of rightfully owned devices may be inhibited from re-use, and therefore end-up in landfills.

5 Gap Analysis

This section provides the gap analysis and is organized into the following subsections:

- Law Enforcement
- Consumers
- Government and Regulators
- Resellers of 2nd Hand Devices
- Database Aggregation
- Shipment of Stolen Devices Overseas

[28] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

- Shortcomings in Existing Solutions

5.1 Law Enforcement

1. Across the US, law enforcement officers may not be aware of the significance of the device identifier (IMEI, MEID, etc.)
2. Procedures to obtain the IMEI or ESN on devices vary among manufacturers and this complicates law enforcement abilities to acquire that information. Also, if the device will not power-on, this further complicates abilities.
3. Across the US, law enforcement officers are not fully aware of how to access information that is in the GSMA IMEI Database.
4. Across the US, law enforcement officers are not fully aware of the capabilities or limitations of third-party databases.
5. Across the US, law enforcement agency polices and practices vary regarding how to deal with stolen device reports (e.g., some agencies may recommend that the carrier be called immediately to shut off service, while other agencies may want to make use of an app such as find my iPhone.)
6. In the US, there is no single law enforcement point of contact or authority on mobile device theft (as compared to the National Mobile Phone Crime Unit in the UK). Part of this may be attributed to our system of government and the fact that mobile device theft is most often a state or local crime, not a federal crime.
7. There is a need for more complete and comprehensive data across the US to include the number of devices stolen, where stolen devices are sold or distributed.
8. Not all device theft is reported to law enforcement. In many cases, customers make the report only to the carrier.
9. Carriers (service providers) have varying hours of operation and may not be available to answer questions, for example at 2:00 AM when a device is stolen.

5.2 Consumers

1. A fragmented system of consumer outreach exists in which no single government agency, group, manufacturer, or carrier providing a uniform and comprehensive outreach program.
2. Consumers don't always report the theft of their devices to law enforcement and/or carriers.
3. Consumers need instructions and clarity of the process and procedures for the reporting of stolen devices.
4. Consumers enabling the anti-theft solutions do not automatically update a centralized database of the IMEI/MEIDs status and do not automatically notify the associated mobile service provider.

5.3 Government and Regulators

1. Irrespective if a solution is developed and implemented, it is possible that there will be 50 different and potentially inconsistent state laws as states struggle with the mobile device theft issue.
2. Currently, there are no consistent practices for traders to reliably avoid purchasing stolen property.

5.4 Resellers of 2nd Hand Devices

1. May be required to adhere to diverse local laws regarding reporting of property taken in.
2. In some case, no laws or best practice exists and resellers are on their own to conduct business as they see fit.
3. Not all ecommerce sites have policies prohibiting the trade of stolen mobile devices.

5.5 Database Aggregation

1. Mobile device information is dispersed across different stakeholder databases such as local/global blacklists, insurance databases, OEM device check services, MEID/IMEI databases, etc. A lookup across more than one database is required to get complete information.
2. Timeliness of information is too long and is dependent on reporting frequency as well as upload/download frequencies of most of the databases. For example, updated blacklist information from the GSMA IMEI Database may be obtained once every 24 hours.
3. Authorized users may not understand the importance of identifiers and how to identify their smartphones.
4. Potential buyers of smartphones do not have access to a complete database to verify that the smartphone is not a stolen mobile device. Potential buyers of smartphones may not understand the importance of identifiers and how to identify their smartphones.

5.6 Shipment of Stolen Devices Overseas

1. There is a lack of information about the number of stolen smartphones that are shipped overseas.
2. There is a lack of device trail of the stolen smartphones shipped overseas.

5.7 Shortcomings in Existing Solutions

1. Stolen device lookup is typically dependent on having access to or knowing the device identifiers. It is also a manual process making it prone to errors.
2. Some mobile network operators in other countries are not using the GSMA IMEI Database. Consequently stolen smartphones in those countries could still be operational.
3. Some US mobile network operators, especially the smaller mobile network operators, do not utilize the GSMA IMEI Database.
4. Device solutions (already and perhaps always possible to circumvent) do not share the device status with database aggregators making it impossible for 3rd parties to adequately check the device status prior to purchase or trade.

6 Cybersecurity and Privacy

This section represents a summary of the analysis performed to address the cybersecurity and associated privacy issues consistent with the FCC Technological Advisory Council Mobile Device Theft Prevention (MDTP) Working Group scope.

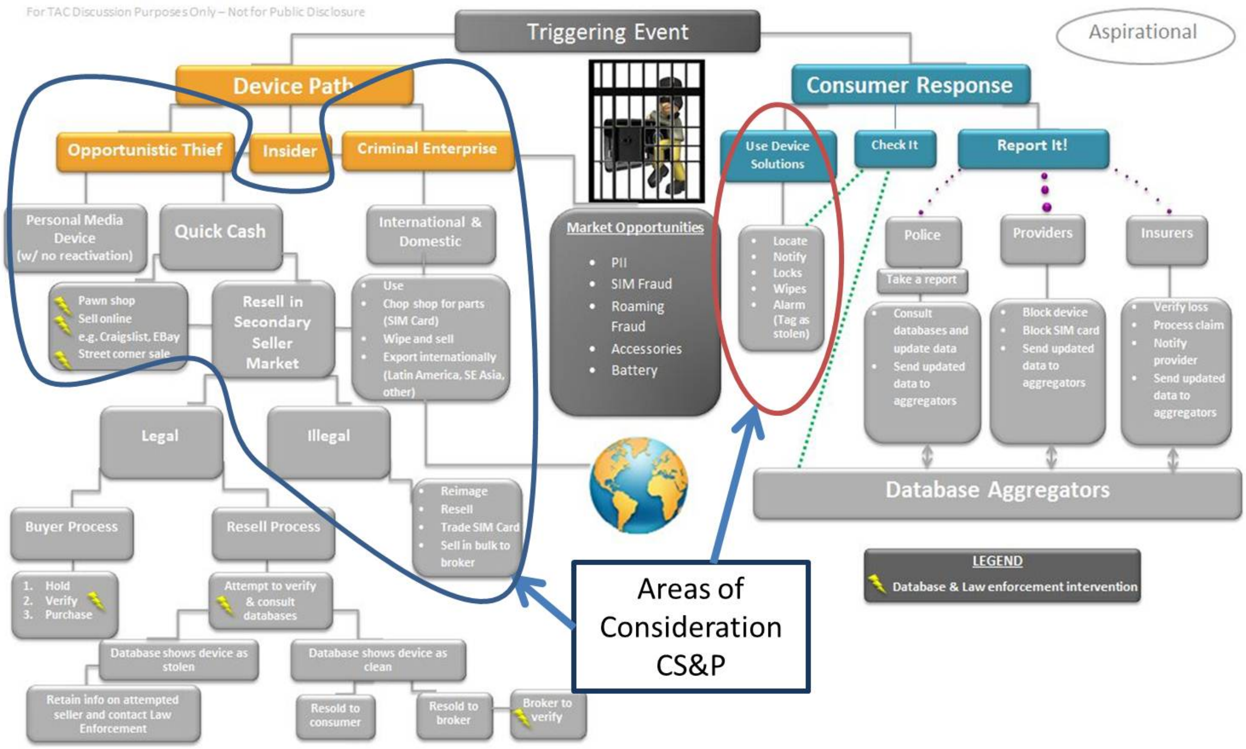


Figure 7: Areas of Consideration for Cybersecurity & Privacy Subgroup

The diagram above represents those areas in the Aspirational view that were studied.

6.1 Solution Categories & Assumptions

6.1.1 Solution Categories

For purposes of this report, anti-theft solution categories are broken down into solutions that are software based, hardware based and solutions that may be network/server/cloud or rely on a mobile device management system (MDM) or some combination of all three. The list below illustrates the three categories and corresponding attributes. The associated Figure describes how the three may be combined and relate to the various functional layers of the smartphone.

1. Software approaches
   - Cost effective to implement
   - Fastest to implement and deliver to market
   - Easy deployment
   - Easy software maintenance and evolution

2. Hardware approaches
    - More costly to implement
    - Longer to implement and deliver to market
    - Harder deployment
    - Harder maintenance and evolution
3. Network/Server/Cloud/MDM based approaches
    - More Secure, approaches not mutually exclusive
    - Cheaper & easier to evolve than hardware alone
    - Device Software/Firmware & Server based
    - Some: Hardware Root-of-Trust, Software/Firmware & Server based
    - Paired Network Access Blocking: IMEI or MEID

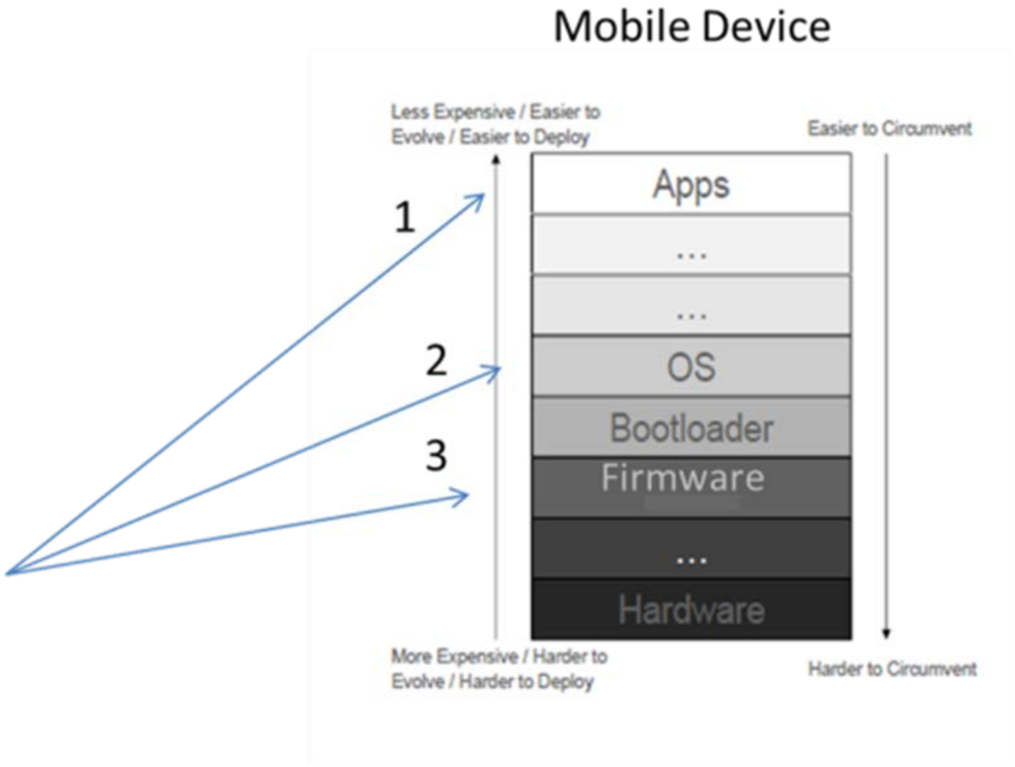

Mobile Device
Less Expensive / Easier to Evolve / Easier to Deploy
Easier to Circumvent
1
2
3
Apps
...
...
OS
Bootloader
Firmware
...
Hardware
More Expensive / Harder to Evolve / Harder to Deploy
Harder to Circumvent

Figure 8: Hierarchy of Mobile Device Theft Solutions

It is important to note that many solutions are systemic in nature and may use all of the above three categories in some fashion. Each one of the above categories addresses different aspects of security and each one adds key functionality since no one category alone is comprehensive. In this scenario the different category elements work collaboratively and provide enhanced security.

6.1.2 Assumptions

In general, anti-theft solutions are assumed to provide a set of capabilities to deter smartphone theft, as well as to help consumers in the event of loss.

There exists a wealth of industry existing solutions[29] that the mobile industry offers today as well as recent industry announcements[30] that highlight ongoing enhancements.

For purposes of the cybersecurity analysis the following non-exhaustive list of capabilities is assumed:

- Remotely Lock/Unlock Smartphone, prevent unauthorized use and network access
- Locate (implicates Privacy considerations)
- Remote Access to Smartphone Data, e.g., Call Log (implicates Privacy & Lawful Access requirements)
- Disable Apps (Non-Emergency & Non-Recovery)
  - Except: Emergency Service Requirements
- Remotely Wipe of the Smartphone
- Prevent Reprogramming
- Re-enable if found or returned to authorized user
  - Restore user data if possible, e.g., Back-Up
- WiFi-only smartphone/use case
- Recovery or reactivation by 3rd Party/Reverse Logistics

6.2 Security & Privacy Considerations

In general, anti-theft solutions help provide a set of capabilities to deter smartphone theft, as well as to help consumers in the event of loss. In the event of theft many players in the mobile ecosystem may interact with the authorized user and include: the network service provider, insurers, the smartphone OEM, the OS provider, the anti-theft solution provider/developer. As outlined, the authorized user has the ability to perform the following actions in order to invoke anti-theft solution functionality to protect the smartphone that is no longer in their possession:

- Typically, the authorized user can access a solution web site and through their account credentials invoke functions to lock, locate or remote wipe the smartphone as they deem appropriate for the circumstances,
- The authorized user will contact the carrier to inform the carrier/network provider that the smartphone is no longer in their possession and thereby block access to network services,
- The authorized user may inform law enforcement of the theft if they suspect the device was stolen, and
- In the event the smartphone is insured the user will also inform the insurer of the event in order to initiate a claim.
- There is a diversity of likely theft reporting points that may be involved in a reported theft by the authorized user. In order to deter theft, data sharing between key theft

[29] http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-apps-for-android-wireless-handsets.

[30] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

reporting points such as network service providers, insurers, OEMs, law enforcement and other relevant industry reporting points is key to ensure up-to-date information and timely visibility of reported theft events. Privacy and security considerations must be taken into account as part of this effort.

6.2.1 Privacy Considerations

As smartphones increasingly contain a wide range of personal data — from health information to payment data to one's intimate photos — device manufacturers and operating system providers may choose to offer encryption solutions such that data on the device is encrypted.

6.2.1.1 Location

Existing industry practices and guidelines[31] are intended to promote and protect user privacy as new Location-Based Services (LBS) are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service – including security and anti-theft mechanisms. Industry guidelines are generally technology-neutral and apply regardless of the technology or smartphone used or the business model employed for LBS (e.g., a downloaded application such as a smartphone anti-theft tool, a web-based service, etc.)

6.2.1.2 Persistent Identifiers Considerations

Personally Identifiable Information (PII) may often be described as information that can be used to identify an individual, such as names, aliases, Social Security Numbers, biometric records, location data, and other personal information that is linked or linkable to an individual. Persistent identifiers may be described as identifiers that can be used to recognize a user over time across different online environments or services. To the extent that the capabilities identified in the detailed analysis may involve persistent identifiers, industry guidelines (e.g., IETF RFC 6973[32]) are intended to address such aspects as data minimization, user control, security, etc.

6.2.1.3 Remote Recovery of Data on Smartphone

Remote recovery of data on the smartphone is the process of accessing data from a smartphone that has its anti-theft function invoked or salvaging data from damaged, failed, corrupted media when it cannot be accessed normally. Through the use of security credentials the authorized user may be able to access the data remotely on the smartphone or alternatively through Cloud or other back-up storage mechanisms. In order to protect personal information on the smartphone, prior to the resale, recycling or donating of a smartphone industry recommends that all information be removed/erased[33].

6.3 Limitations

Anti-theft solutions have limitations as outlined below.

6.3.1 Social Engineering/Trick-Consumer

Social engineering, in the context of information security, refers to psychological manipulation of people (tricking the consumer) into divulging confidential information (e.g., contacting the

[31] As an example see: http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf?sfvrsn=0.
[32] IETF RFC 6973, Privacy Considerations for Internet Protocols, July 2013, http://tools.ietf.org/html/rfc6973.
[33] http://files.ctia.org/pdf/CTIA_DataErase.pdf.

user and masquerading as a customer care agent to solicit security credentials or other personal information). Once the hacker or cybercriminal has access to the confidential information, they may be in the position to defeat the anti-theft tool by masquerading as the legitimate user to disable the tool, or block access to it by the legitimate user.

6.3.2 Physical Attacks: “Faraday Cage”, Theft of Briefcase, Purse, Luggage

It is important to note that while many solutions effectively help protect the smartphone that has been lost or stolen, there remains physical attacks on the smartphone through isolating it from communicating via its radio(s) link (i.e., cellular or WiFi) that are a limitation. One such example attack is simply wrapping the smartphone in aluminum foil, otherwise known as a Faraday Cage. In this scenario the smartphone is unable to receive the command to invoke the anti-theft functions on the smartphone because the radio(s) have been compromised by the physical attack.

Other attacks could also include scenarios where the smartphone is collateral associated with the theft of other articles such as a briefcase, purse, or luggage.

6.3.3 Component Value – i.e., Striping Smartphone for Parts

It is important to note while many solutions effectively reduce the marketable value of a smartphone that has been lost or stolen, there remains a residual component value, e.g., screen, battery, precious materials.

7 Consumer Outreach

The section of the report provides information regarding consumer outreach on the problem of mobile device theft. This section is organized into the following subsections:

- Review of Current Consumer Outreach re: Stolen Phones
- Review of Best Practices of Other Consumer Outreach Initiatives
- Review of Data on Consumer Behavior
- Review of the Effectiveness of Other Public Safety Campaigns
- Identification of Key Stakeholders for Outreach

7.1 Review of Current Consumer Outreach re: Stolen Phones

7.1.1 Government Stakeholders

7.1.1.1 FCC

As an initial step, the subgroup researched information that is already available to consumers on the topic of stolen phones. The subgroup began its research by going to the websites of the FCC, DOJ, DHS and others. The subgroup found that while the FCC had good information on their website, the others represent an opportunity. They had information in general about crimes, but nothing specific to smartphones.

The FCC has a history of taking the steps necessary to aid law enforcement in their fight to deter the theft of smartphones. On April 10, 2012, CTIA – The Wireless Association® (“CTIA”), in coordination with the FCC and the major city Police Chiefs, announced a voluntary commitment by CTIA[34] and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data. These are described more fully below.

1. **Implement databases to prevent reactivation of stolen smartphones.** Wireless providers will work to initiate, implement and deploy database solutions, using unique smartphone identifying numbers, designed to prevent smartphones reported by their customers as stolen from being activated and/or provided service on their own networks. Using unique GSM smartphone identifying numbers, GSM providers will develop and deploy a database designed to prevent GSM smartphones reported as stolen from being activated or provided service. By October 31, 2012, U.S. GSM providers will implement this database so that stolen GSM smartphones will not work on any U.S. GSM network. In addition, U.S. providers will create a common database for LTE smartphones designed to prevent smartphones that are reported stolen by consumers from being activated or provided service on any LTE network in the U.S. and on appropriate international LTE stolen mobile smartphone databases. This database will be completed by November 30, 2013.

2(A). **Notify consumers of features to secure/lock smartphones with passwords.** By April 30, 2013, smartphone makers will implement a system to notify/inform users via the new smartphones upon activation or soon after of its capability of being locked and secured from unauthorized access by setting a password.

2(B). **Educate consumers about features to secure/lock smartphones with passwords.** By December 31, 2012, smartphone makers will include information on how to secure/lock new smartphones in-box and/or through online "Quick Start" or user guides.

3. **Educate consumers about applications to remotely lock/locate/erase data from smartphones.** Wireless providers will inform consumers, using communications including email or text messages, about the existence of – and access to – applications that can lock/locate/erase data from smartphones. Providers will also educate consumers on how to access these applications, including those that are easy-to-find and preloaded onto smartphones. Substantial progress on this will be made by December 31, 2012; it will be completed by April 30, 2013.

4. **Educate consumers about smartphone theft, protections and preventative measures.** By July 1, 2012, the wireless industry will launch an education campaign for consumers on the safe use of smartphones and highlight the solutions one through three by using a range of resources, including a public service announcement and online tools such as websites and social media.

With regard to the FCC website, when you search the term "stolen phones" it brings you to a section entitled "FCC Consumer Facts: Stolen and Lost Wireless Devices"[35]. This section has important and valuable information for consumers about how they can safeguard against wireless device theft, protect the data on their phones, what to do if their device is lost or stolen including contacting their carrier and, if their device is stolen to contact their police department. The information provided also has Steps to Smartphone Security for Windows, Apple iOS, Blackberry and Android.

[34] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

[35] http://www.fcc.gov/guides/stolen-and-lost-wireless-devices.

In 2012, the FCC released a blog during the 2012 Holiday Season[36] to remind folks to be mindful of their devices and tips on how to do so during the holiday season. In advance of Independence Day, the FCC did a joint Consumer Advisory[37] with the D.C. Metropolitan Chief of Police Cathy Lanier with tips on how to be "smart" about your smartphone. They are:

> **Record device information.** Mobile devices have unique numbers (IMEI or MEID numbers) that can identify devices if they are stolen. You should record the IMEI or MEID number, serial number and MAC/Wi-Fi address and store it in a safe place. This information is usually found under the "Settings" menu on the "About" screen. Additionally, screenshot functions make it easy to capture this information and send it to an email account.
>
> **Before you go out**:
>
> - Find the IMEI or MEID number on your mobile device.
> - Send yourself a screenshot of it: iOS (Apple), Android, Blackberry, and Windows.
>
> **Be aware of your surroundings**. Many mobile device thefts are crimes of opportunity. Using your device in public, particularly on public transit, or leaving it out in the open makes it easier for thieves to grab the device and run.
>
> **Treat mobile device theft like credit card theft.** Mobile devices frequently contain sensitive financial and personal information.
>
> **Report all mobile device thefts immediately** to your wireless carrier and local law enforcement.
>
> **Set a password/PIN and use the lock screen function**. The password/PIN and lock screen functions on devices make it more difficult for thieves to use your stolen device and access your personal data. These functions should be set up as soon as you purchase a new device. (CTIA – The Wireless Association® has instructions for setting up a password on Android, Blackberry, Apple and Windows devices at http://blog.ctia.org/2012/03/22/passwords-mobile-device.)
>
> **Consider using mobile security apps.** Mobile security apps can be useful in locating and recovering stolen devices. Common features include the ability to remotely track, lock or erase your personal data on your mobile devices. Some apps also allow you to remotely trigger an alarm on the device or take a photo of the thief. CTIA provides a list of mobile security apps[38].

[36] http://www.fcc.gov/blog/fcc-and-public-private-partners-launch-smartphone-security-checker-help-consumers-protect-mobil.

[37] http://www.fcc.gov/document/tips-protecting-your-mobile-device-theft.

[38] http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data.

Regularly back up photos and data. Photos, videos, contacts, email and other data you would want to keep if your device is stolen should be backed up regularly on a computer, USB drive or cloud service.

Locate, lock and erase. You should inform law enforcement of your mobile security app that might help locate and recover the device. In addition, the remote lock feature can prevent thieves from using your stolen device. It may be best to remotely erase your personal data on the device if you believe it will not likely be recovered or if it contains sensitive financial, health or work information.

For More Information

- Visit http://www.fcc.gov/guides/stolen-and-lost-wireless-devices and http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data for more information about protecting your mobile devices.
- A Spanish-language version of these consumer tips is also available. http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/cómo-detener-el-robo-de-teléfonos-inteligentes-y-proteger-sus-datos.

Additionally, on June 19, 2014 the FCC held a workshop that brought together a comprehensive and extensive group of national and international experts in the field to delve into Mobile Device Theft Prevention[39]. Shortly thereafter, the FCC established a working group, at the direction of FCC Chairman Wheeler, within the TAC and charged it with making actionable recommendations to the Commission (to include Consumer Outreach) by the end of 2014. The FCC also established an official docket for the filing of consumer comments to inform and supplement the initiative, including consumer outreach efforts.

The FCC has also developed a Consumer Guide to Stolen and Lost Mobile Devices[40].

7.1.1.2 Department of Justice

A review of the Department of Justice website provides online resources on various topics under its Consumer Information Program. It breaks down information by subject. It does not, however, have any information on stolen phones. The subgroup believes that, at a minimum, tools and tips as provided by the FCC should be on this website.

7.1.1.3 Federal Bureau of Investigations

While the FBI takes part in a Federal Trade Commission led effort called "National Consumer Protection Week" and has tips and tools for consumers on how to "Be Crime Smart", there is no specific information about stolen phones on their website.

[39] http://www.fcc.gov/events/fcc-announces-workshop-focus-prevention-mobile-device-theft.
[40] http://www.fcc.gov./guides/stolen-and-lost-wireless-devices.

7.1.1.4 Department of Homeland Security

The subgroup saw similar results as above when the subgroup conducted a search on the DHS website. Although there is information about what to do if your phone is stolen, it is embedded in a document entitled "Cyber Threats to Mobile Phones"[41]. As such, it is not easy to find and should be more prominently displayed.

7.1.2 Industry – Mobile Service Providers, Manufacturers, Others

The U.S. wireless industry has been proactively educating consumers about device theft and protecting personal information for some time. As previously mentioned, on April 10, 2012, CTIA, in coordination with the Federal Communications Commission and the major city Police Chiefs, announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data. This included a commitment to:

- Notify consumers of features to secure/lock smartphones with passwords.
- Educate consumers about features to secure/lock smartphones with passwords.
- Educate consumers about applications to remotely lock/locate/erase data from smartphones.
- Educate consumers about smartphone theft, protections and preventative measures.

All of these were accomplished by CTIA and the participating companies. Here are some of the steps that were taken by the participating companies to get the message out:

- Launching "vanity" URLs that provide detailed information to consumers concerning security tips, reporting a stolen smartphone and buyer protection options.
- Sending welcome e –mails that are sent after a new phone activation to encourage the use of passwords.
- Text messaging campaigns with pertinent information.
- Utilizing social media to get the word out.
- Using sales and support teams to reinforce adding smartphone passwords after activation and guidance on downloading apps that help to protect devices and personal information.
- Messages on monthly bills or inserted into bills encouraging the use of passwords and the use of applications to remotely track, lock and wipe smartphones.
- Messages in customer newsletters about steps to take before and after a customer's phone are missing.
- Instructions for setting a password added to in-box user guides.
- Workshops online and in stores intended to educate consumers on a wide range of topics including security measures.
- Ensuring the customer care representatives are trained to help customers set passwords on their devices.

CTIA also took steps, in accordance with the agreement, to educate consumers about the tools available to them. This included the production of a public service announcement entitled, "The

[41] https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf.

Five Stages of Losing a Smartphone" which is attention-grabbing and includes tips for consumers. This PSA is also on the website[42] that CTIA created which has all of the tips and tools for consumers for both before and after their smartphones are either lost or stolen. Also, prominently featured on CTIA's main homepage[43] is detailed information on steps CTIA and participating companies are taking to deter smartphone theft.

AT&T recently launched a ***Be Aware: Protect Your Phone*** campaign which was announced at an event in Minneapolis, MN. The event was attended by elected officials and representatives from the Minneapolis Downtown Improvement District, Minneapolis Police Department, Metro Transit Police Department and Minneapolis Public Schools. The event was covered by local media and was shared on social media by some of the attendees and the Minneapolis Downtown Council featured the campaign on their website.

Be Aware is a multi-channel public awareness campaign that will span outdoor media, Facebook advertising, social media, downtown handouts and promotions within Minneapolis Public Schools:

- Ads are now running on the interiors of buses on the primary downtown route provider, the interiors of light rail trains into downtown and around campus, and on kiosks at Nicollet Mall in downtown Minneapolis.
- The campaign also includes targeted advertising on Facebook, as well as a Twitter campaign that promotes regular tips on how to protect your phone.
- The Minneapolis Police Department and the Minneapolis Public School District are also providing promotional partnership support.
  - All public high schools in Minneapolis are receiving Be Aware campaign materials to distribute to students, including cell phone screen cleaners and informational handouts.

While much good work continues to be done by the wireless industry, the Consumer Outreach subgroup highlights this campaign as it illustrates how a local campaign can be initiated in coordination with local law enforcement, business groups and schools.

7.1.3 Law Enforcement

The Consumer Outreach Subgroup focused on activity here in the Unites States in the District of Columbia as well as efforts taken by law enforcement in the UK.

In the UK

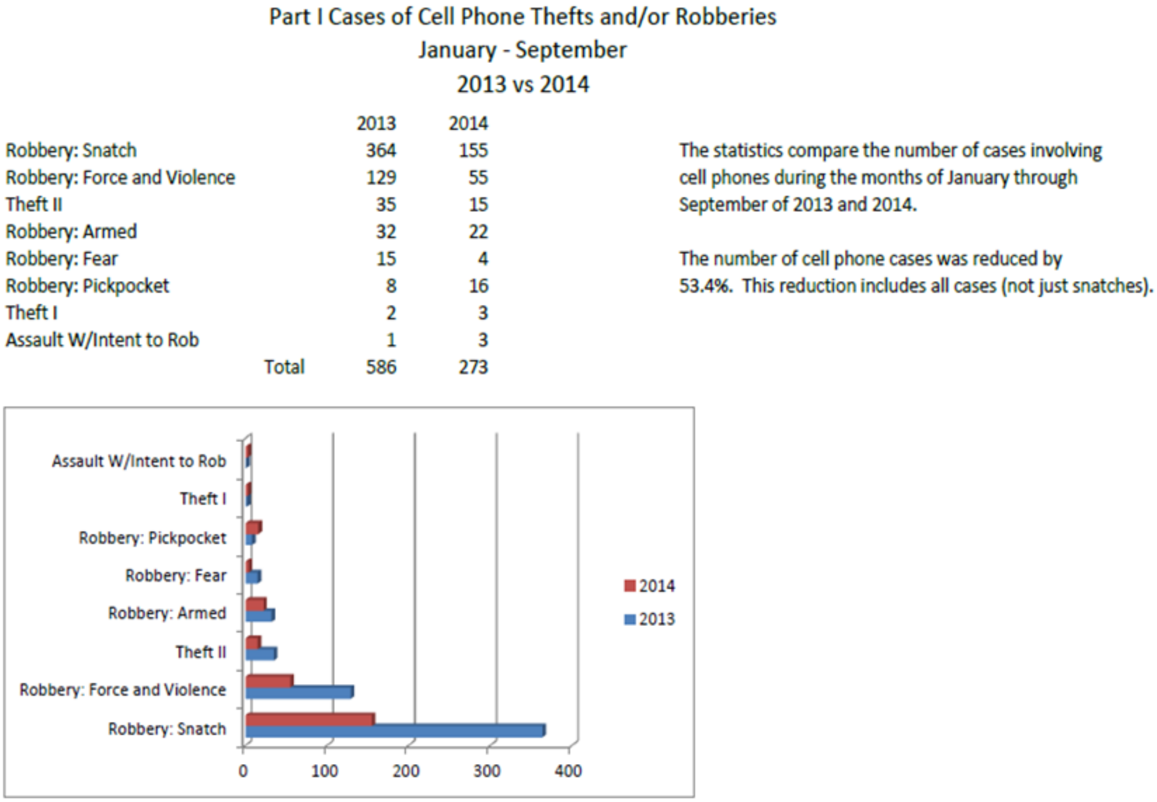
In the UK, there is currently a tool in place where consumers can register their smartphones prior to theft or loss. To date, 18 million people have registered their phones. Although there is no such tool currently here in the US, there are some lessons to be learned from what law enforcement has done there. In the UK law enforcement runs regular promotions such as property marking days or visiting universities and colleges at the start of the term to educate students. They also make good use of social media such as Twitter and Facebook (https://twitter.com/search?q=immobilise.com&src=typd) and reinforce the message through interviews and TV appearances.

[42] www.beforeyouloseit.org.
[43] http://www.ctia.org/.

In the U.S.

Here in the U.S., the District of Columbia engaged in a consumer awareness campaign from which best practices can be developed. For example, they used posters on buses, public buildings, and at community meetings (see below). They recorded a PA, produced public service announcements that have been used in metro stations, trains, buses, etc. In addition, Metro Transit Police (MTPD) routinely reinforce rider vigilance by engaging media through the release of redacted CCTV footage to illustrate how these crimes happen, release of suspect BOLO's (pictures of suspects or wanted subjects) and general reminders on social media. Upon detecting an increase in snatch-theft crimes last year, Metro Transit invited the media in for a widely covered news conference to discuss concerns and urge riders to "get their heads out of their phones". One thing that should be noted is that they refresh the PSAs approximately every 90 days. They believe this helped improve the effectiveness of the campaign. Additionally, they distributed flyers on stolen phones entitled "late night travel tips" and "cell phones" throughout the National Capital Region District with a focus on metro stations that have historically been "high crime" stations. Finally, they used media opportunities to get the message out to the public.

As to the effectiveness of the consumer outreach, while the results cannot be solely attributed to the campaign itself, the MTPD reports that in the first 6 months of 2014, thefts and/or robberies involving cell phones were reduced by over 50% from the same time period in 2013. In the first 14 days of October 2014 there were 12 cases involving cell phone theft. In 2014, the MTPD averaged 30.3 cases per month involving cell phones. The MTPD reported continued declines, no increases in cell phone cases even after the release of the new iPhone early in the month.



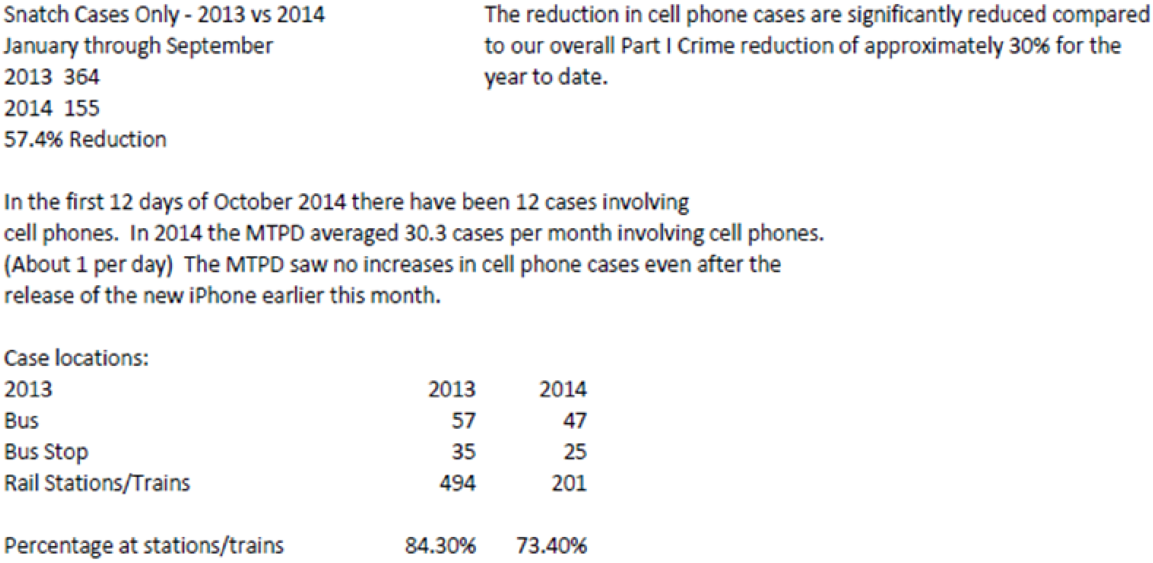
Part I Cases of Cell Phone Thefts and/or Robberies
January - September
2013 vs 2014

	2013	2014
Robbery: Snatch	364	155
Robbery: Force and Violence	129	55
Theft II	35	15
Robbery: Armed	32	22
Robbery: Fear	15	4
Robbery: Pickpocket	8	16
Theft I	2	3
Assault W/Intent to Rob	1	3
Total	586	273

The statistics compare the number of cases involving cell phones during the months of January through September of 2013 and 2014.

The number of cell phone cases was reduced by 53.4%. This reduction includes all cases (not just snatches).

Figure 9: MTPD Cell Phone Thefts/Robberies Statistics 2013 vs. 2014



Snatch Cases Only - 2013 vs 2014
January through September
2013 364
2014 155
57.4% Reduction

The reduction in cell phone cases are significantly reduced compared to our overall Part I Crime reduction of approximately 30% for the year to date.

In the first 12 days of October 2014 there have been 12 cases involving cell phones. In 2014 the MTPD averaged 30.3 cases per month involving cell phones. (About 1 per day) The MTPD saw no increases in cell phone cases even after the release of the new iPhone earlier this month.

Case locations:

2013	2013	2014
Bus	57	47
Bus Stop	35	25
Rail Stations/Trains	494	201
Percentage at stations/trains	84.30%	73.40%

Figure 10: MTPD Snatch Cases Only Statistics 2013 vs. 2014

The District of Columbia Metropolitan Police Department (MPD) has done an extensive education campaign to help combat theft of smartphones. Their approach has been three-fold: 1) information for consumers **before** their smartphones are stolen; 2) information for consumers

after their smartphones are stolen; 3) **rewards** for the public who might be aware of and willing to report those stealing smartphones. As shown with the other types of outreach programs that the subgroup has looked at, the program is targeted to individuals on the community level.

In the case of the MPD, their department is divided into seven different districts. In each of those districts, there is a Community Outreach officer. It is these employees, along with all officers in the districts that are working to get the word out to the aforementioned populations. In each of those districts, there are ways that they do so. They use Yahoo groups where citizens can sign up to get information from the MPD. They also use Twitter, press conferences and community meetings (which are held regularly). Through these outlets they share flyers with consumers about how to protect their electronics.

See:
(http://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/page_content/attachments/Laptops%20and%20Personal%20Electronics.pdf,

http://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/page_content/attachments/Protecting%20Your%20Gadget%20-%20Reward%20Poster.pdf.

Also, there is a particular focus on protecting electronics during the holiday season which is the time when electronics are on the minds of consumers who are buying them or receiving them. They also distribute helpful information about protecting your smartphones, but also what to do if your smartphone is lost or stolen, and it includes the telephone numbers of the major carriers as well the numbers for the local police.[44]

The MPD has also developed 4x6 palm cards that instruct people to be aware of their surroundings with tips for reducing their chances of being a victim of a crime. It notes that you should protect your electronics by not displaying them. These palm cards are distributed to the members of the MDP and they distribute them throughout the community. This is a particularly good tool when an officer sees someone talking on their phone and not being aware of their surroundings. They have a particularly eye catching poster to remind their citizens that smartphones have value. Entitled “What Thieves See,” these posters are distributed for display on public buildings and elsewhere throughout the District.[45] (see below):

[44] http://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/page_content/attachments/Reporting-Bricking%20a%20Stolen%20Phone.pdf.

[45] http://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/What%20Thieves%20See%20%28Series%29.pdf.

THIS IS HOW THIEVES
SEE YOU ON THE STREET.

BE AWARE WHEN YOU USE
YOUR ELECTRONICS.

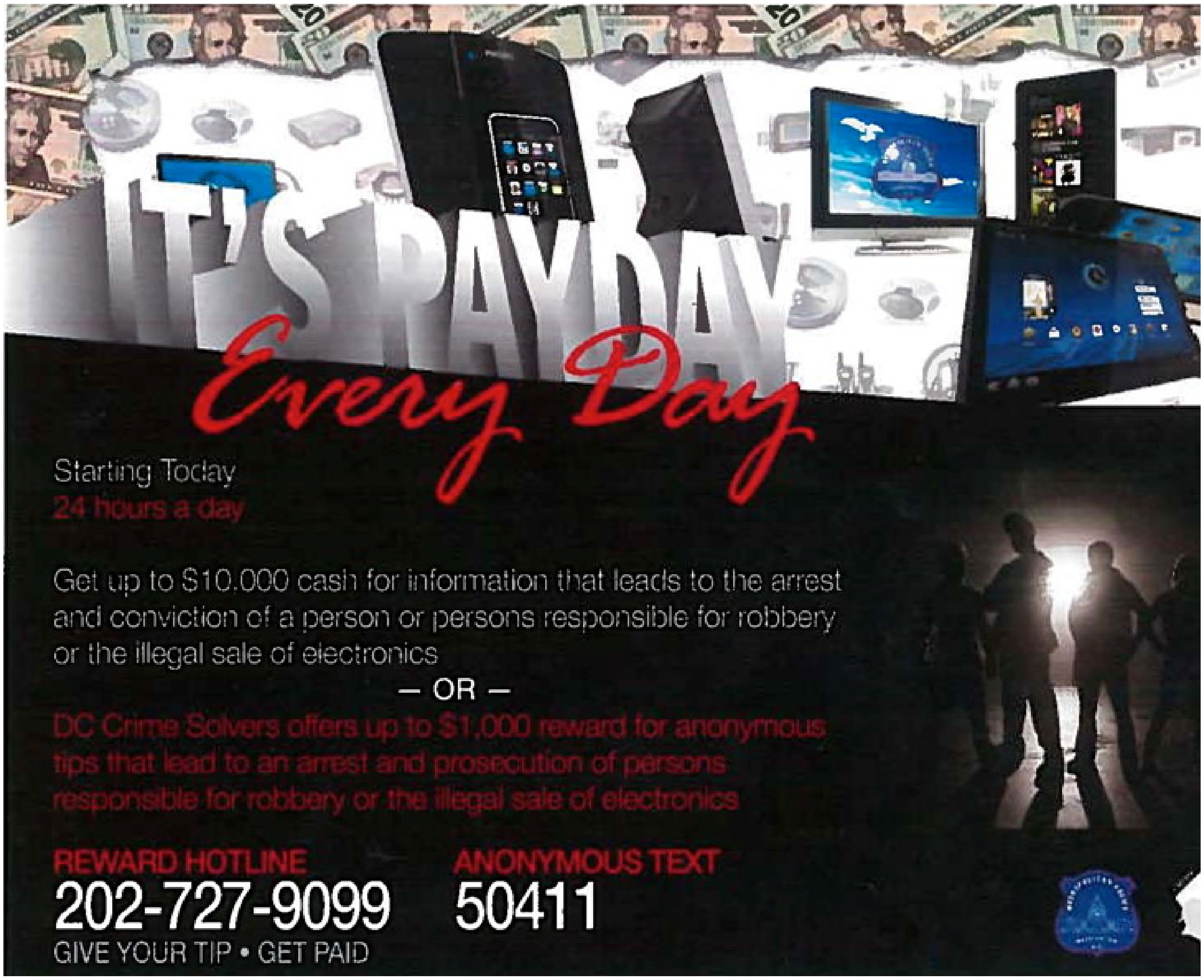
For more ways to protect yourself, visit WWW.MPDC.DC.GOV/SAFETY

THE DISTRICT
OF COLUMBIA
One City, One Government, One Voice

VINCENT C. GRAY
Mayor

CATHY L. LANIER
Chief of Police

Finally, the MPD has a program where they reward those who may have information that leads to an arrest or conviction of a criminal who robs an electronic device. This card (see below) is distributed throughout the District.


IT'S PAYDAY
Every Day

Starting Today
24 hours a day

Get up to $10,000 cash for information that leads to the arrest and conviction of a person or persons responsible for robbery or the illegal sale of electronics

— OR —

DC Crime Solvers offers up to $1,000 reward for anonymous tips that lead to an arrest and prosecution of persons responsible for robbery or the illegal sale of electronics

REWARD HOTLINE
202-727-9099

ANONYMOUS TEXT
50411

GIVE YOUR TIP • GET PAID

Notably, while these efforts are commendable and have been a great tool in producing good results, what is missing to date is a coordinated, uniform consumer outreach campaign nationwide. A national consumer outreach campaign which is uniform and organized would likely produce favorable results across the county.

7.2 Review of Best Practices of Other Consumer Outreach Initiatives

Consumer outreach is a dynamic process that typically requires a multi-faceted approach. Consumers assimilate messages in a variety of ways. In some instances the messaging is national in scale from organizations like the Ad Council. In other instances a consumer may be best reached in a targeted message from their local community like law enforcement or other public stakeholders. There are outreach initiatives that offer examples of how to engage consumers on an issue that needs a broad based response.

Recycling offers a great example especially as it relates to e-waste. Getting plastic out of the waste stream and back in productive use was a challenge. However, e-waste presented a new set of issues. Consumer habits with regard to electronics were different than with plastic bottles. E-waste also presented potentially harmful substances into the waste stream. It was very important to reach consumers on not only the importance of the issue but on how they can handle their end-of-life products.

The messaging on e-waste has come from public stakeholders, private entities and public/private partnerships. The broadcasting of information has ranged from the national to the local level. The methods of communication have ranged from television, print, internet and radio.

The Ad Council with its nationwide recognition has created engaging messages for recycling in general. On the Ad Council website they feature additional information on specific types of recycling like e-waste and connect you with organizations like the Consumer Electronics Association (CEA). CEA in turn provides a feature where a consumer can enter their zip code and find options for recycling in their area. In this instance a consumer is engaged, educated, and ultimately has the tools to take action locally.

Here is the Ad Council's link to "Greener Gadgets": http://www.iwanttoberecycled.org/search and the CEA "Greener Gadgets" site with zip code search: http://greenergadgets.org/.

Another significant effort in recent years has been around the dangers of texting and driving. There have been a number of partnerships in addressing consumers. The State Attorneys General partnered with NHTSA and produced a campaign called "Stop the Texts, Stop the Wrecks"[46]. Private companies have started their own campaigns which utilize broader based print ads as well as direct to the customer with bill inserts.

In each of these cases, national to local organizations have reached consumers with multiple layers of information that start with awareness and then provided the tools for action. This dynamic approach is needed to reach a very diverse marketplace and each of these instances demonstrates the need to get a widespread issue down to a local consumer level.

7.2.1 Government

7.2.1.1 Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau has online financial education services for adults, students and kids. Their website is very well-organized and can serve as a model for a website about stolen smartphones. They have a call center that has quick pick and short wait times. Of note, they market other programs during on-hold times. Another important part of this education campaign is the use of social media; they use blogs as an important source of information. Finally, Consumer Financial Protection Bureau officials tour the US to raise the profile of various agency programs and consumer awareness[47].

7.2.1.2 Office of the Comptroller of the Currency

The subgroup looked at the education/consumer outreach program offered by the Office of the Comptroller of the Currency which features online information on consumer financial protection issues. They have formed the Consumer Assistance Group (CAG) which processes questions

[46] http://www.stoptextsstopwrecks.org/#home.

[47] http://www.consumerfinance.gov/#inside.

and complaints about consumer issues[48]. They also offer links to related agencies and organizations that help consumers. Of note, while they have lots of information in the form of press releases and news, it is not always in a consumer friendly format.

7.2.2 Industry

The subgroup took a look at successful campaigns conducted in the private sector. While not directly on point as they were selling a product, there are some important lessons to be learned.

In an article entitled "8 Do's and Don'ts for More Effective Ad Campaigns"[49], the author stressed the need to clearly define your goals and expectations. The question is "What are we trying to accomplish by when and how much will this cost?" While the audience for the article is financial institutions and those who advise them, the message is a good one for many industries. Also, it is important that people know what the benefit is from buying the product. This line of thinking directly correlates to the discussion at hand. Consumer outreach on the loss or theft of smartphones must be tied to the benefit that the consumer will get by protecting themselves and taking the correct actions if their smartphones are lost or stolen. The article also illustrates the importance of a website. It is noted that when companies engage in campaigns they often overlook their websites. It should be substantively and visually consistent with the campaign.

One thing that is evident is the importance of social media in any campaign. In an article published in 2010[50], the author listed what he believed to be the top 10 best media marketing campaigns of all time. In it, he highlighted when Evian launched its 'Roller Babies' video in July 2009 as part of its 'Live Young' campaign, and instantly gained success. The video notched up 27,000,000 views on the official YouTube video and an estimated 61,000,000 views across the web in total, making it the most popular online advertisement ever. He noted that the most interesting aspect of Neilson's research was the fact that 95% of the people in France (one of the countries where the advertisement was first launched) who viewed the video online had not seen the ad on TV. This illustrates the need for online video and social media in general to augment traditional media efforts.

7.2.3 Law Enforcement

The FBI conducted a National Consumer Protection Week Link to National Consumer Protection Week 2014. This took place on March 2-8 and it marked the 16th annual National Consumer Protection Week, which is a Federal Trade Commission-led education initiative. Members of the FBI participated in the week—offering tips and guidelines to help consumers, as they say on FBI.gov, "Be Crime Smart." On the website, there is a wealth of material to help consumers get informed and to protect themselves. Everything from information on protecting your kids, computers, and workplace to a list of types of fraud schemes and e-scams and even how to report this type of criminal activity is on the site. Specifically, there are links to:

- National Consumer Protection Week Website (http://www.ncpw.gov)
- Scams & Safety (http://www.fbi.gov/scams-safety)
- Frauds from A to Z (http://www.fbi.gov/scams-safety/frauds-from-a-to-z)
- Common Fraud Schemes (http://www.fbi.gov/scams-safety/fraud)

[48] http://www.occ.gov/topics/consumer-protection/index-consumer-protection.html.
[49] http://thefinancialbrand.com/31471/8-tips-for-more-effective-advertising-campaigns/.
[50] http://acquisitionengine.com/top-10-best-social-media-marketing-campaigns-all-time/.

- E-Scams & Warnings (http://www.fbi.gov/scams-safety/e-scams)

7.3 Review of Data on Consumer Behavior

The subgroup looked primarily at research commissioned by CTIA-The Wireless Association® which was done by Harris Interactive entitled "Cybersecurity Research" and was published in January 2013[51].

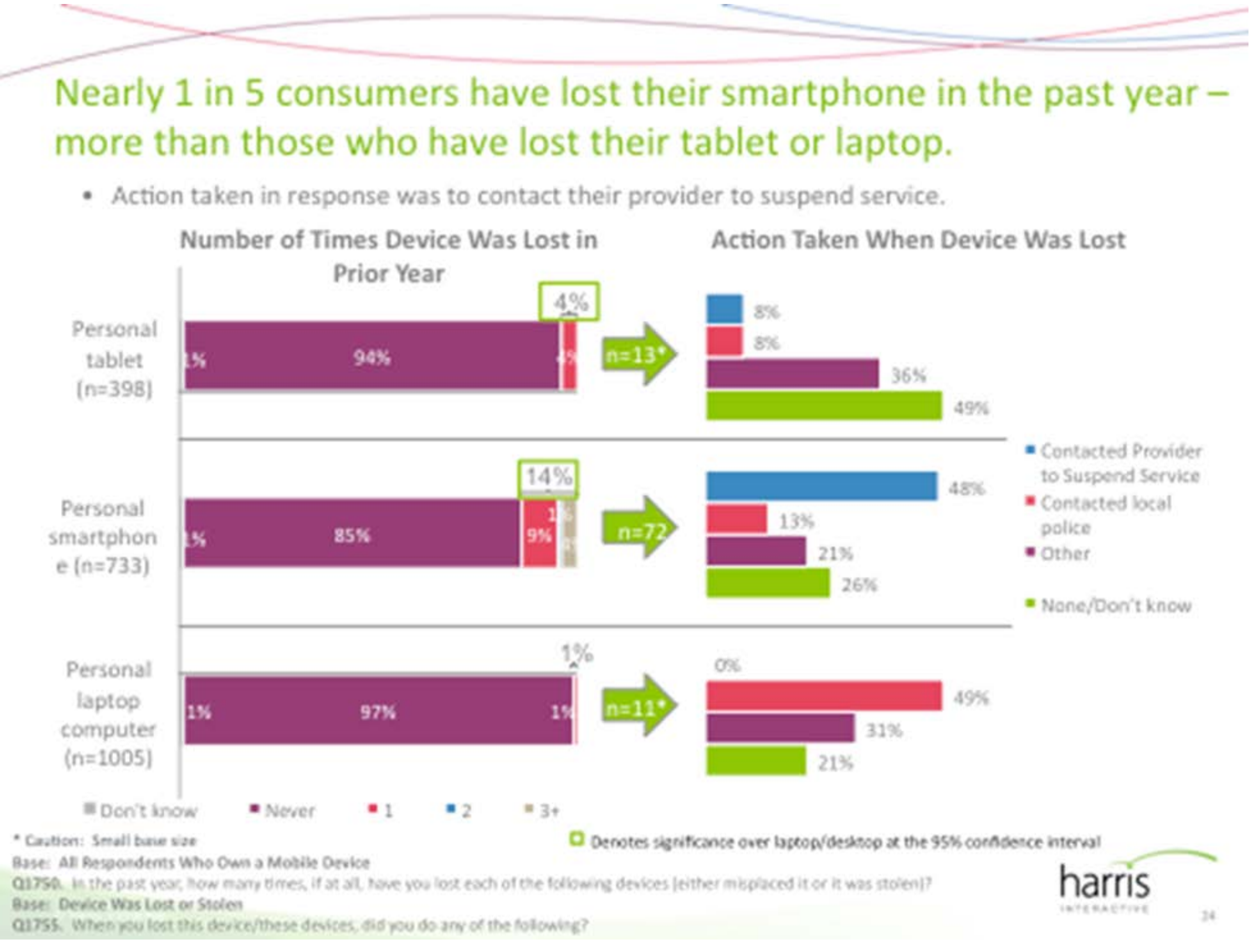
The research was conducted both over the phone and online and was conducted with 1,516 adults ages 18+ who own and use a cell phone or smartphone. While the main focus of the research was in the area of Cybersecurity, there are some statistics and findings that are relevant to this report.

For example, three quarters of consumers believe the responsibility to keep their device safe falls mostly to them. The subgroup believes that this is important when considering how effective a consumer outreach campaign might be. If most consumers believe that the responsibility to keep their phones safe lies with them, then it would logically flow that they would be more inclined to listen to a message about how to keep their smartphones safe.

The research disclosed that approximately one half use a password or PIN to access their smartphone, but this is much less than with computers. This is certainly an area of opportunity with respect to messaging to consumers. Similarly, there is an opportunity with respect to consumers who report a lost or stolen phone to their service provider. Of the percentage who have lost or had their smartphone stolen, almost half contacted their wireless service provider. There is another opportunity here as well to ensure that any messaging covers this as well.

The research disclosed that approximately one half use a password or PIN to access their smartphone, but this is much less than with computers. This is certainly an area of opportunity with respect to messaging to consumers. Similarly, there is an opportunity with respect to consumers who report a lost or stolen phone to their service provider. Of those who have lost or had their smartphone stolen, almost half contacted their wireless service provider (Harris slide 20 pictured below):

[51] http://ctia.it/18Lzlv3.



Nearly 1 in 5 consumers have lost their smartphone in the past year – more than those who have lost their tablet or laptop.

- Action taken in response was to contact their provider to suspend service.

* Caution: Small base size

Denotes significance over laptop/desktop at the 95% confidence interval

Base: All Respondents Who Own a Mobile Device

Q1750. In the past year, how many times, if at all, have you lost each of the following devices (either misplaced it or it was stolen)?

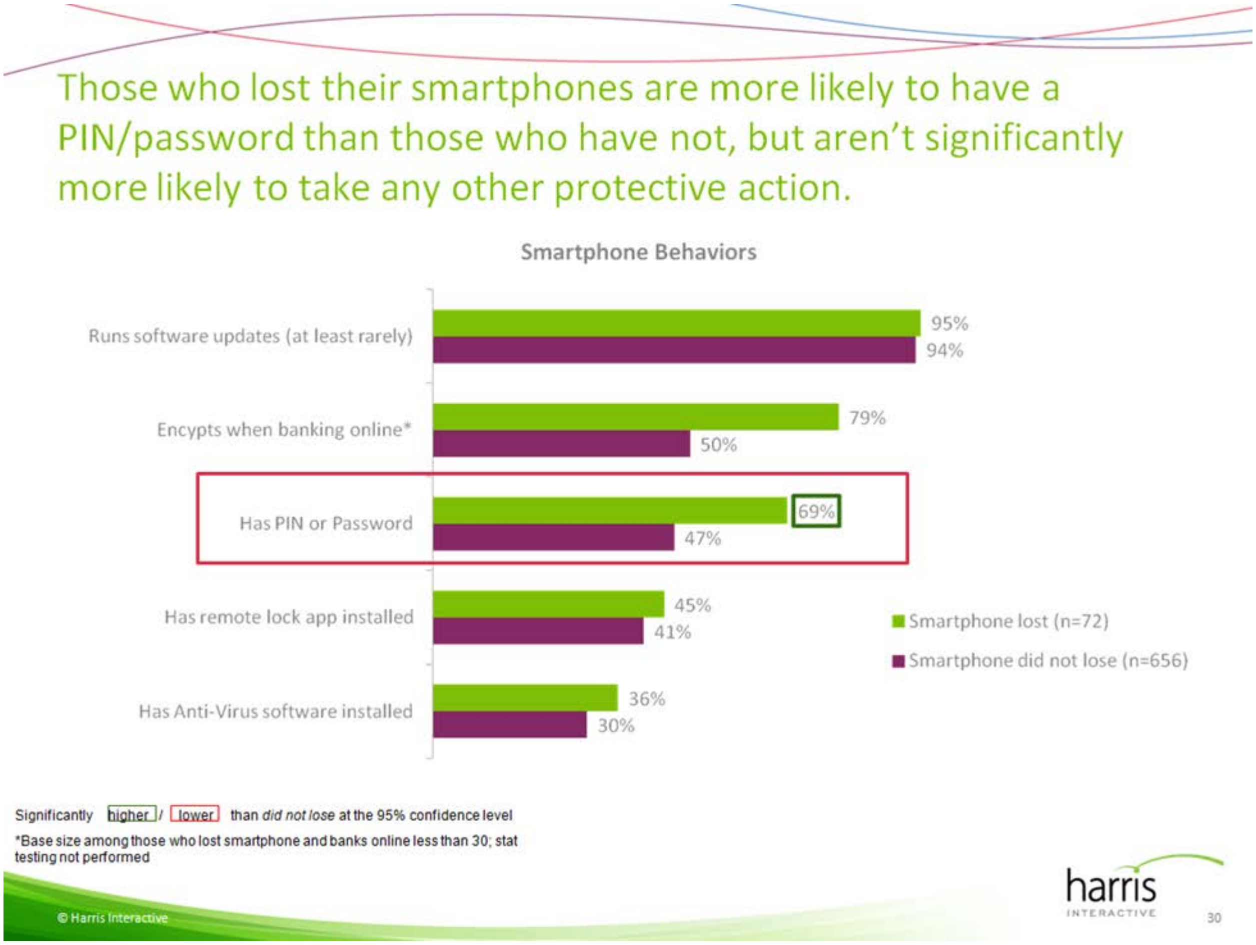
Base: Device Was Lost or Stolen

Q1755. When you lost this device/these devices, did you do any of the following?

This emphasizes the perception that service providers already play a key role in the eyes of consumers, and are ideally placed to continue to leverage the existing relationship with consumers to promote safety and prevention with their customers.

The research also showed that consumers are more apt to protect themselves against tangible threats (like loss of a mobile device) versus intangible threats (hacking, malware, etc.) and, although not a majority, many consumers have an app that remote locks, locates and wipes. (Note that this represents the consumers who are aware of this capability being present, as some consumers may not be aware of built-in capabilities).

Finally, while those who have lost their smartphones are more likely to have a PIN/password, they aren't necessarily significantly more likely to take any other protective action. (Harris slide 30, pictured below):



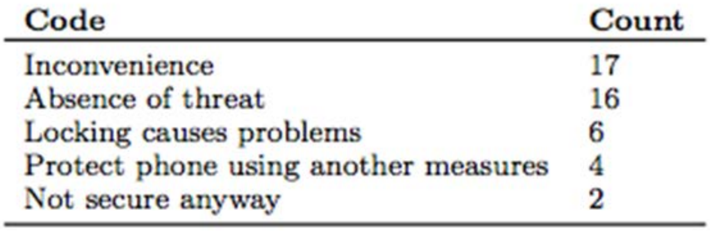
Those who lost their smartphones are more likely to have a PIN/password than those who have not, but aren't significantly more likely to take any other protective action.

Significantly higher / lower than *did not lose* at the 95% confidence level

*Base size among those who lost smartphone and banks online less than 30; stat testing not performed

© Harris Interactive

Other recent research studies, such as "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception"[52] and "Modifying Smartphone User Locking Behavior"[53] looked at the reasons for consumer use/non-use of device locking mechanisms. These smaller studies revealed that, somewhat contrary to the Harris study, consumers' perception of risk when it comes to mobile devices diverges from the more classical PC or laptop and is viewed as being at lower risk.



Code	Count
Inconvenience	17
Absence of threat	16
Locking causes problems	6
Protect phone using another measures	4
Not secure anyway	2

Table 10: Reasons for not using a code-based locking mechanism of field study participants.

[52] Harbach, et. al.; https://www.usenix.org/system/files/conference/soups2014/soups14-paper-harbach.pdf.

[53] Van Bruggen, et. al.; https://cups.cs.cmu.edu/soups/2013/proceedings/a10_VanBruggen.pdf.

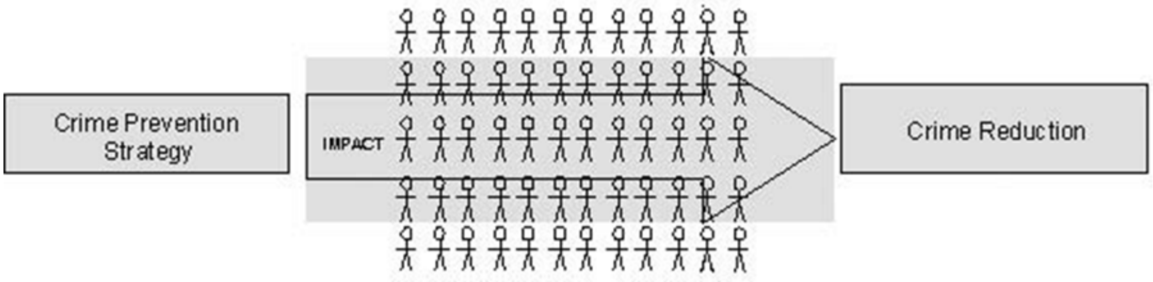
It was also identified that it is difficult to convince a non-user of device locking mechanisms to start using such a mechanism, with inconvenience and absence of threat being stated as the primary reasons. This perhaps presents an opportunity for OEMs and service providers to continue to highlight the variety of locking mechanisms available to consumers with varying levels of complexity and security to meet their various needs.

7.4 Review of the Effectiveness of Other Public Safety Campaigns

As the subgroup was considering consumer behavior and areas of opportunity for a consumer outreach effort, the subgroup decided to take a look at some of the research about the effectiveness of other consumer outreach campaigns. For example, the Center for Public Safety Initiatives released a report in April, 2012 entitled "Media Campaigns and Crime Prevention: A Review of the Literature"[54]. In it, the author concludes that "while the literature behind prevention publicity campaigns offers mixed support, those that support prevention publicity campaigns make it clear that effective campaigns must have a clear and concise mission statement that the general public should be able to understand, appreciate and rally behind, a clear means of evaluating the effectiveness and the success or failure of the program." He goes on to state, "poorly planned or poorly executed campaigns may, in addition to wasting valuable resources, serve to increase the fear of crime, harm police and community relations, among other unintended consequences".[55]

The Center for Problem Orientated Policing produced a paper on Crime Prevention Publicity Campaigns[56]. While it was published in 2006, the subgroup believes that much of what is in the report can still be effective guidance today. In it the author states that "informing a community about a crime problem, introducing target-hardening measures, or warning of increased police patrols can lead to an increase in self-protection or a decrease in offenses."[57]

The report goes on to state: "The figure below shows the impact of a stand-alone (no publicity component) crime prevention strategy aimed at offenders. While the initiative does manage to deter or help police apprehend a segment of the offending population, many offenders remain unaffected. This is partly because in this kind of scenario, the crime prevention benefits are limited to those who have heard about the operation or who have been directly affected by it.



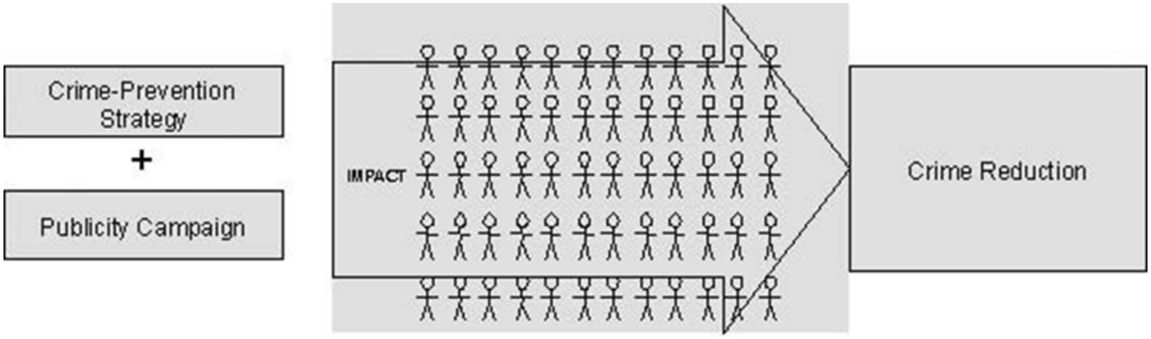
[54] http://www.rit.edu/cla/criminaljustice/sites/rit.edu.cla.criminaljustice/files/docs/WorkingPapers/2012/2012-02.pdf.

[55] http://www.rit.edu/cla/criminaljustice/sites/rit.edu.cla.criminaljustice/files/docs/WorkingPapers/2012/2012-02.pdf.

[56] http://www.popcenter.org/Responses/crime_prevention/print/.

[57] http://www.popcenter.org/Responses/crime_prevention/print.

In the following figure, a complementary publicity campaign advertises the same crime prevention strategy. Through the advertisement, however, a bigger segment of the population hears about the strategy, and more crime reduction results.



Publicity campaigns in crime prevention operate much like advertising campaigns in the private sector. Commercial advertisements are intended to persuade a target audience to buy a particular product by publicizing information meant to appeal to that audience. Effective commercial advertisements therefore sway customers to change their behavior, usually by buying something. When it comes to crime prevention, the same dynamics are at work. Those targeted by the intervention (offenders and victims alike) need to be exposed to information that will influence their future decision-making processes. The key is to devise proper campaigns and to match the message to the audience. There are numerous ways to use publicity, and agencies can benefit from succinct and properly designed campaigns to support crime prevention efforts. This guide's purpose is to help local police plan and implement effective publicity campaigns by exploring their benefits and pitfalls."

In the report the author delineates the differences between "victim-oriented campaigns" and "offender-oriented campaigns". The MPD campaign is a good illustration of both. They have targeted the victims but by offering a reward for arrest of conviction of the offenders, they are also targeting the offenders. The report notes that victim campaigns should focus on specific crimes and should be carried out in small geographic regions to be most effective. Specifically the report states:

"However, victim campaigns that focus on specific crimes and are carried out in small geographic regions seem to be more effective.[58] They seem to have more success because people feel the messages are more relevant to their immediate situation than are generic warnings about crime. A good example of this type of campaign was carried out by the North Brunswick Police Department in New Jersey. In 1998, the department decided to address auto thefts through a multimedia publicity campaign. The campaign included television public service announcements (PSAs), newsletters from the mayor's office, crime prevention brochures, community bulletin boards, and local billboards, among other measures. The effort also included the donation of free Clubs® from local businesses. By attending local community functions, the police could reach many residents, effectively disseminating specific crime prevention information. One out of

[58] Johnson, S., and K. Bowers (2003). "Opportunity Is in the Eye of the Beholder: The Role of Publicity in Crime Prevention." Criminology and Public Policy2(3):497–524.

three residents reported some contact with the campaign, and of those, nearly all adopted the proposed crime prevention measures, significantly reducing auto crimes.[59]

Sometimes, victim publicity campaigns reduce crime because they alert offenders that the police are doing something new or are paying more attention to the problem.[60] While warning offenders is not an intended part of the campaign, the message still reaches them."[61]

The summary of the section on victim-oriented crimes states:

- Victim-oriented campaigns work best when carried out in small geographic areas.
- Victim campaigns should focus on specific crime types.
- General victim campaigns are rarely successful in changing prevention behaviors.
- Many victim campaigns fail to reach the intended audiences with the message.
- Timeliness and relevance are key to campaign success.
- The campaign may have an indirect positive effect of warning offenders.

The subgroup also looked at an evaluation done on the effectiveness of the "Take a Bite Out of Crime" or "McGruff" crime prevention campaign initiated in 1979[62].

The summary states:

> "A large-scale formal survey evaluation indicated that McGruff seems to have had some success in promoting various aspects of crime prevention competence among a fairly wide range of citizens. A national survey of 759 crime prevention practitioners revealed that the McGruff campaign has served as a centerpiece for a host of allied preventive efforts at local, statewide, and national levels. A survey of 53 television station public service managers indicated considerable receptivity to the McGruff public service announcements. **McGruff's effectiveness may be tied in part to the use of formative research in its design, and to the integration of interpersonal and community-level support with the media components.**"[63] (emphasis added)

7.5 Identification of Key Stakeholders for Outreach

To adequately identify key stakeholders for outreach, the subgroup looked at the current educational programs regarding stolen smartphones as well as the data that was available as to the effectiveness of the education campaigns. For consumers, it is most effective to get the messaging to them on the local level but consistent messaging should also be a goal. Messaging about how to protect your smartphone and your data and what to do when your smartphone is lost or stolen need to be consistent and requires a clearly defined process for reporting thefts and a non-technical explanation of tools available for consumers regarding theft prevention.

[59] Simmons, T., and G. Farrell (1998). Evaluation of North Brunswick Township Police Department's Community-Oriented Policing Project To Prevent Auto Crime. North Brunswick, N.J.: North Brunswick Township Police Department.

[60] Simmons, T., and G. Farrell (1998). Evaluation of North Brunswick Township Police Department's Community-Oriented Policing Project To Prevent Auto Crime. North Brunswick, N.J.: North Brunswick Township Police Department.

[61] http://www.popcenter.org/Responses/crime_prevention/print

[62] http://eric.ed.gov/?id=ED308555.

[63] http://eric.ed.gov/?id=ED308555.

FCC – The FCC should act as the facilitator, the coordinator and the aggregator for any consumer education campaign. The FCC essentially can be the "hub" from which the elements of the consumer outreach campaign can be developed. This is not to suggest that the other key stakeholders are not critical to the success of any type of outreach campaign. However, the subgroup believes that the FCC should play a central role in the development of the campaign. The FCC can also play an important role in encouraging other agencies such as DOJ and the FBI to include tools and tips on their websites and to incorporate them into their other consumer education campaigns.

Law Enforcement- As previously mentioned, the evidence gathered by the sub-group indicates that the message is most effective coming from local law enforcement. The campaign initiated in the District of Columbia as well as that done in Minneapolis, MN are certainly examples of such campaigns. Local law enforcement is the best "messenger" to deliver the consumer outreach campaign. They have access to consumers through local community events such as fairs, community meetings, high school and college assemblies, etc. They can place posters on public buildings, on trains or buses. However, there is a role for national law enforcement to play. The sub-group identified a few agencies (FBI, DOJ, and DHS) that don't have any information for consumers on how to protect their smartphones and what to do if they are lost or stolen. Finally, there may be an opportunity to make use of the vast numbers of security personal throughout the country. The International Association of Industrial Security is a global organization of more than 38,000 security practitioners who are charged with protecting assets, property, and/or information. This could be a valuable resource for consumer outreach.

Industry – As noted previously, the industry has done much to educate consumers about the issue of stolen phones (see Section 7.1.2) The Working Group encourages the industry to maintain the efforts that they have undertaken. This messaging is most important as it will augment the messaging that is being delivered by local law enforcement. The industry is also encouraged to work with the FCC in the development of the "kit" that would be used by local law enforcement. Outreach by OEM's should involve straightforward and a non-technical explanation of anti-theft tool implementations on various, individual platforms and instruction on disabling an anti-theft tool upon device trade-in or sale. For successful mobile service outreach, providers must continue to leverage consumer relationships to sufficiently communicate theft prevention messages while maintaining a consistent message across various media platforms used by each service provider.

Finally, outreach must extend to the secondary market vendor community and facilitate the extension of the outreach through these vendors to consumers. In order for secondary market vendor outreach to be effective, they must understand and explain the benefit of participation in device tracking databases, as well as providing messaging to consumers in trade-in/buyback programs. Any outreach has to include secondary market vendors to insure all consumers in the value stream are reached with the key messaging regarding kill switch implementations.

8 Recommendations

The recommendations from the MDTP Working Group are organized into the following four areas:

- Actionable Recommendations for the FCC
- Guidelines to Law Enforcement
- Guidelines to Industry

- Further Work

8.1 Actionable Recommendations for the FCC

Top Priority Recommendations:

Recommendation 1.1: The FCC TAC recommends that the FCC establish a common national framework for smartphone anti-theft measures and explore the basis for preemption. This is critical to:

- Ensure participation of all stakeholders including law enforcement, industry, States and US territories,
- Ensure consistency and clarity in requirements, terminology, and timeline,
- Avoid possible fragmentation across States and US territories,
- Through economies of scale, provide the most efficient distribution of anti-theft measures throughout the base of users,
- Provide a technically-reasoned and achievable goal for industry,
- Prevent conflicting or growing requirements that may impact the ability of the industry to deliver solutions uniformly to consumers in the United States and US territories in a timely manner, and
- Act as a single point to process feedback and shape future revisions.

Recommendation 1.2: The FCC TAC recommends that Part I of the CTIA "Smartphone Anti-Theft Voluntary Commitment"[64] and existing laws in California and Minnesota be used as input into the development of the common national framework of Recommendation 1.1 since there is an existing, broad industry commitment and active development efforts to deliver solutions by July 2015.

Note: The common national framework should be applicable only to retail consumer devices.

Recommendation 1.3: The FCC TAC recommends that the FCC remain technology neutral in any common national framework pertaining to mobile device theft prevention, allowing the industry to identify and evolve the technical approaches for solutions to meet the functional requirements for smartphone anti-theft capabilities without limiting innovation by solution providers in a competitive market. In the event that such industry driven technical standards, protocols, procedures, and related requirements are standardized, recognized accredited industry bodies that have well defined Intellectual Property Rights (IPR) policies shall be utilized to form the standards.

Note: Smartphone anti-theft deterrence has many aspects, including wireless operator network-based solutions, use of global databases, and device-based solutions. A comprehensive technology solution does not involve a single solution, but will require solutions across networks and devices. The technologies to support mobile device theft deterrence include network-based solutions such as the Equipment Identity Register (EIR) and carrier fraud prevention systems and using global databases to block blacklisted devices from accessing service on the network. Mobile device based solutions are applications that allow remote locking, locating, and

[64] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

wiping data from the mobile device if the device is connected to a network and can be accessed through a communications channel to enable the owner of the device to perform such functions. These mobile device based solutions may be device or OS vendor specific, or may be carrier or third-party available applications that perform the functions required.

Recommendation 1.4: The FCC TAC recommends that CSRIC, in coordination with appropriate industry standards bodies (e.g., GSMA-NA Regional Interest Group, ATIS), be tasked with developing policies, methods or procedures for law enforcement to obtain device identifiers from smartphones in their possession that are under theft investigation.

Recommendation 1.5: The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.

Note: Device identifiers are typically available on smartphones either through a label on the device (which may be under the back cover or under the battery), or available through a menu option on the screen. This recommendation is to define standards, methods, and procedures for obtaining such identifiers from the device even if the device is locked or disabled, and may include a combination of physical and electronic methods for obtaining the identifier.

Recommendation 1.6: The FCC TAC recommends that CTIA convene a joint Law Enforcement, carrier, and wireless industry task force to define a consumer outreach process to encourage consumers to initially report smartphone thefts to their carrier.

Note: As part of the carrier customer care dialogue with the consumer, the carrier customer care should encourage the consumer to notify the local law enforcement of the smartphone theft and provide supportive information to the consumer specifically the IMEI/MEID. This does not imply any obligation on the carrier to report a stolen device to law enforcement on behalf of the consumer.

Recommendation 1.7: The FCC TAC recommends that the FCC TAC/MDTP Working Group continue the joint task force between key theft reporting points such as carriers, insurers, law enforcement, and other relevant industry reporting points to define a process for the capture of comprehensive data (e.g., number stolen, make, model, distribution, device trail) relative to smartphone thefts and encourage increased data sharing to ensure up-to-date information and timely visibility of reported theft events. The FCC should encourage greater use of the existing device registry databases.

Note #1: If current tools are determined to be insufficient by law enforcement, desired capabilities for tools need to be documented and rationalized for industry consideration.

Note #2: Privacy and security considerations must be taken into account as part of this effort.

Note #3: Study should include minimization of the risk of false positives, redundancy of information, risk of spoofing/cloning and other risks.

Recommendation 1.8: The FCC TAC recommends that the FCC should seek input from consumer organizations which survey how consumers are utilizing the anti-theft solutions and related security capabilities available on their devices.

Recommendation 1.9: The FCC TAC recommends that the FCC develop a "kit" to be shared with local law enforcement agencies for the purpose of educating consumers on how they can protect their smartphones, their data and what to do if their smartphone is lost or stolen.

> Note: The message should be concise and consistent. The kit could include such things as a short video, handouts, flyers, posters etc. and could also include the CTIA developed PSA to help get the message out. Outreach recommended to be done by local law enforcement is defined in Section 8.2.

Recommendation 1.10: The FCC TAC recommends that the FCC encourage work with the smartphone re-seller industry to form a voluntary code of practice to promote consistent due-diligence behaviors and interaction with law enforcement to prevent the inadvertent trade of stolen devices. The voluntary code of conduct should also address the treatment and disposition of smartphones that are reported stolen. It is further recommended that the effort be taken up in the next CSRIC.

Recommendation 1.11: The FCC TAC recommends the FCC reach out to the following organizations to effectuate a comprehensive and effective consumer outreach effort:

a. The Major Cities Chiefs Association.
b. The International Association of Chiefs of Police.
c. The National Sheriffs Association.
d. The National Crime Prevention Council.
e. International Association of Industrial Security (ASIS).

> Note #1: The most important stakeholder in consumer outreach on the topic of stolen smartphones is local law enforcement. The success in the UK and in the District of Columbia is certainly evidence of the fact that people listen to their local law enforcement officials. What is missing in the U.S. is a consistent, national message that is delivered by local law enforcement. There is also an opportunity through ASIS to connect security practitioners.

> Note #2: Law enforcement should seek out opportunities to educate their communities regarding stolen phones using the kit to be developed by the FCC (see Recommendation 1.9). The community education opportunities should include distributing information in high crime areas or at gathering places in their towns, villages and cities such as attending community meetings, visiting college campuses, seeking out interview opportunities on radio or television.

Recommendation 1.12: The FCC TAC recommends that the FCC make use of pre-recorded answering of calls to their information line and during on-hold times, reminding consumers that they can protect their information and their smartphones and direct them to the FCC Website for tips and tools.

> Note: The CC TAC Group believes that the best and most effective messenger here is local law enforcement. However, the FCC can augment that outreach.

Recommendation 1.13: The FCC TAC recommends that the FCC Chairman encourage his international counterparts to become more engaged on the Mobile Device Theft Prevention issue to:

- Promote adoption of shared network-based solutions (e.g. GSMA IMEI Database) globally, which will extend the reach of device blocking and increase deterrence of device trafficking, and
- Promote greater coordination and cooperation on this global issue.

Additional Recommendations:

Recommendation 1.14: The FCC TAC recommends that the FCC promote greater consumer awareness of existing anti-theft measures through the efforts of the Consumer Advisory Committee.

Recommendation 1.15: The FCC TAC recommends that the FCC work with CTIA and GSMA's North American Regional Interest Group to encourage additional operators to participate in the April 10, 2012 voluntary commitment[65] to take certain actions (e.g., GSMA IMEI Database) to help law enforcement deter smartphone theft and protect personal data. This voluntary commitment includes the technology aspect of operators using the GSMA IMEI Database or CDMA database to blacklist devices reported stolen, and then using those blacklists across operators to deny service on the network using network-based technology solutions such as an Equipment Identity Register or other fraud prevention systems available on carrier networks.

Recommendation 1.16: The FCC TAC recommends that the FCC augment their consumer outreach efforts by using social media, blogs during key times of the year (the holiday season, back-to-school with an emphasis on college students, etc.)

Recommendation 1.17: The FCC TAC recommends that the FCC encourage other federal agencies to place tips and tools on their websites, or link to the FCC website.

Recommendation 1.18: The FCC TAC recommends that the FCC continue the efforts of the TAC to address the further work items defined in Section 8.4 *Further Work*.

8.2 Guidance to Law Enforcement

Recommendation 2.1: The FCC TAC recommends that a single law enforcement point of contact be established to serve as a clearinghouse of information and expertise on mobile device theft, much like the National Mobile Phone Crime Unit in the United Kingdom.

Note #1: This single point of contact would be the location where local law enforcement agencies could retrieve information and best practices.

Note #2: An example of the information available from this clearinghouse would be the information contained in Section 3.2.2.3.

Note #3: This point of contact should also act as a coordinating body for law enforcement existing tools awareness program.

Recommendation 2.2: The FCC TAC recommends that an education campaign be developed with the assistance of the GSMA-NA Regional Interest Group and CTIA and coordinated with

[65] U.S. Wireless Industry Announces Steps to Help Deter Smartphone Thefts and Protect Consumer Data, April 10, 2012 http://www.ctia.org/resource-library/press-releases/archive/deter-smartphone-thefts-and-protect-consumer-data.

law enforcement associations for dissemination to police officers to educate them on important aspects relative to smartphone theft.

Note #1: Examples of topics for the education campaign include the following:

- The significance of the smartphone identifiers such as IMEI and MEID.
- Importance of accurately recording smartphone identifiers [i.e., IMEI, MEID and ESN (Electronic Serial Number)] in theft cases, take steps to improve accuracy and data integrity, and checking them against available databases.
- How to acquire the smartphone identifiers from the smartphone.
- How to access to the GSMA IMEI Database.
- The use of third-party databases.

Note #2: An example of a law enforcement association would be the International Association Chiefs of Police (IACP).

8.3 Guidance to Industry

Recommendation 3.1: The FCC TAC recommends that CTIA convene an ongoing study of how to make anti-theft solutions easy for consumers to understand and use, potentially providing consistent messaging on next steps when theft occurs.

Recommendation 3.2: The FCC TAC recommends that solutions providers and the ecosystem involved in reverse logistics (carriers, device recyclers, device resellers, etc.) ensure that the solution providers have enacted a mechanism for reverse logistics providers. The approaches to such mechanisms vary by solution provider, but as long as there are manual or automated means to successfully achieve disabling protection, industry stakeholders should have flexibility in determining the right approach. A prescriptive recommendation on the technical approach to reverse logistics limits innovation by solution providers in a competitive market.

Recommendation 3.3: The FCC recommends that CTIA convene a joint Law Enforcement, carrier, and wireless industry task force, in cooperation with consumer groups (e.g., Consumers Union), to define a process for law enforcement to repatriate a stolen smartphone if found or recovered.

Note: This process may include consumers being encouraged to voluntarily register their device identifiers.

Recommendation 3.4: The FCC recommends that CTIA in coordination with the carriers and wireless industry develop a method and procedure for consumers to be able to lookup smartphone IMEI/MEID status.

Note: This is similar to what is available on the Canadian web site[66].

Recommendation 3.5: The FCC TAC recommends that smartphone anti-theft solution providers offer a mechanism for consumers to check enrollment status of a device in the solution.

Recommendation 3.6: The FCC TAC recommends that the industry continue its work educating consumers about how they can protect their data and their smartphones to augment what the FCC and law enforcement is doing.

[66] http://www.protectyourdata.ca/check-the-status-of-your-device-in-canada/.

Recommendation 3.7: The FCC TAC recommends that the industry continue to share its best practices with the FCC and work with the FCC as needed on the consumer outreach program.

Recommendation 3.8: The FCC TAC recommends that the GSM Association's North American Regional Interest Group and CTIA jointly develop a voluntary process to report to the FCC statistics on devices reported lost or stolen over a 12 month period, using the CWTA report to the Canadian Radio-television and Telecommunications Commission as a model.

Recommendation 3.9: The FCC TAC recommends that the GSM Association's North American Regional Interest Group, along with other appropriate stakeholders, develop a best practices and guidelines on how to measure and report on blacklisted devices going forward, including guidelines to establish consensus in terms of blacklisting policies to ensure consistency of what is blocked and measured.

8.4 Further Work

Recommendation 4.1: The FCC TAC recommends the FCC TAC/MDTP Working Group perform ongoing study of potential new, measurable risks to public safety that requires future assessment and consideration by industry.

Recommendation 4.2: The FCC TAC recommends the industry TAC/MDTP Working Group perform ongoing study and monitoring of the dynamic and changing threat environment.

Recommendation 4.3: The FCC TAC recommends the FCC TAC/MDTP Working Group perform ongoing study and consideration of new and emerging technologies and global standards for the purpose of aiding in the mitigation of smartphone theft.

> Note: This ongoing study should include but not be limited to the examination of the usage of identifiers and making them more resistant to change by outside parties, if required.

Recommendation 4.4: The FCC, working with the FCC TAC/MDTP Working Group, should provide an annual assessment of smartphone theft and assess the effectiveness of the measures undertaken to combat theft. In addition, the FCC should assess the effectiveness of tools provided to law enforcement including the rate of participation in law enforcement in using such tools.

Appendix A: Glossary

AMPS **Advanced Mobile Phone System**

API **Application Programming Interface**

Authorization The process of determining the level of access approved for a user. Both anonymous and authenticated users can have permissions assigned to them, authorizing access to different capabilities. For example, the owner of a smartphone might be authorized full access but a support agent assisting the user remotely might only be authorized to run diagnostic tools.

Cellular Network-based Anti-Theft Solution A technical solution that executes on a cellular network to prevent a specific device from accessing that cellular network. The unique identifier (i.e., IMEI, MEID, or ESN) of the target device is added to a black list that disallows future connections. This prevents the device from being able to access a specific cellular network, but it remains capable of connecting to other cellular networks, wireless networks, or being used offline – access to Essential Features is not prevented. Some cellular network providers share their black lists with other providers to further restrict a device's potential to access cellular networks.

CDMA **Code Division Multiple Access**

CDR **Call Detail Record**

CEA **Consumer Electronics Association**

Credit muling Credit fraud in which a customer of a bank uses his or her own name and information to obtain high-value loans with no intention of paying them back[67]. Also known as first party fraud.

CSRIC **Communications Security, Reliability and Interoperability Council**

CTIA **Cellular Telecommunications Industry Association**

CWTA **Canadian Wireless Telecommunications Association**

Cyberthreats Potential vulnerabilities that bad actors can exploit to compromise data, extract information or interrupt services.

DDOS **Distributed Denial of Service**

An attempt to make network/server resources unavailable through overload and congestion. The attacks are generally efforts to temporarily or indefinitely interrupt or suspend access to services from devices connected to the Internet.

EIR **Equipment Identity Register**

[67] http://www.creditcards.com/glossary/term-credit-muling.php#ixzz3IcgMJ7ar.

Encryption The process of encoding information so it can only be read by authorized parties; decoding encrypted information requires a key that is in the possession of an authorized user. Encryption can be applied to local data to prevent unauthorized access on devices and it is also used in secure network communications (typically over SSL) to protect against eavesdropping or unauthorized alteration during transmission.

ESN **Electronic Serial Number**

A unique number placed on and within a mobile device by its manufacturer. It is used within a mobile wireless network to identify and confirm the device. The ESN standards were defined by TR45 for AMPS, TDMA and CDMA mobile devices.

Essential Features Ability to use the smartphone for voice communications, text messaging, and the ability to browse the Internet, including the ability to access and use software applications. “Essential features” exclude the functionality needed for the operation of the anti-theft solutions, the ability of the smartphone to access emergency services by a voice call or text to emergency services (e.g., “911” in the United States), the ability of a smartphone to receive wireless emergency alerts and warnings, and the optional ability to call an “In Case of Emergency number (ICE)” pre-designated by the owner.

FCC **Federal Communications Commission**

Feature Phone A class of mobile devices describing low-end phones with limited capabilities as compared to smartphones. These devices typically offer calling, texting, basic multimedia, and basic internet features, but generally have limited support for third-party applications and are built on special-purpose operating systems with limited capabilities.

Flash Flashing a mobile device refers to the operation of overwriting the firmware and/or operating system on the device, typically with the same or a newer version of the one already installed. It differs from a reset in that flashing is typically done while connected to a computer that transfers the software image via USB and, unlike a reset, the version is not necessarily the same after the process completes.

GSM **Global System for Mobile communications**

GSMA **GSM Association**

Hard Reset / Factory Reset / Master Reset Restoration of a smartphone to the default software settings of the smartphone, the smartphone will be in a state ready for use on a carrier network.

ICE **In Case of Emergency**

An optional feature provided by some smartphones that allows a locked smartphone to call a number pre-programmed by the owner. This is a type of emergency number that is intended to be accessible even when the rest of the smartphone’s functionality is not.

IETF **Internet Engineering Task Force**

IMEI **International Mobile Equipment Identifier**

A unique decimal number placed on and within a mobile device by its manufacturer. It is used within a mobile wireless network to identify and confirm the identity of a mobile device. The IMEI standards are defined by 3GPP in 3GPP TS 23.003.

IMSI **International Mobile Subscriber Identity**

A unique identification used to identify the user of a cellular network. It is usually a 15 digit number, but can be shorter. The first 3 digits represent the mobile country code (MCC), which are followed by the mobile network code (MNC), either 2 digits (European standard) or 3 digits (North American standard). The remaining digits are the mobile identification number (MIN).

IoT **Internet of Things**

Jailbreaking Jailbreaking is the process of bypassing technical restrictions placed on iOS-based devices. It allows users to unlock the bootloader to enable changing the operating system, successfully sideload apps that are not approved by the App Store, and run applications with administrator-level privileges. Jailbreaking goes beyond the concept of “rooting” which primarily focuses on obtaining administrator-level privileges.

Kill Switch A smartphone-based anti-theft measure that, once initiated and successfully executed on the smartphone, renders the essential features of the smartphone inoperable by an unauthorized user. An authorized user can reverse the restriction of functionality by authenticating with credentials accepted by the anti-theft solution.

LBS **Location-Based Services**

LEA **Law Enforcement Agency**

LTE **Long Term Evolution**

Malware Malicious software designed to access or alter data or interfere with device or network functions. It may manifest itself as worms, Trojan Horses, spyware, adware, apps, data files or web pages with executable scripts.

MDTP **Mobile Device Theft Prevention**

MEID **Mobile Equipment Identifier**

A mobile equipment identifier (MEID) is a globally unique number identifying a physical piece of CDMA mobile station equipment. The number format is defined by the 3GPP2 report S.R0048.

MIN **Mobile Identification Number**

The MIN, more commonly known as a wireless phone number, uniquely identifies a mobile device that is paired with a mobile wireless network. The MIN is dialed from other wireless or wireline networks to route a connection to a specific mobile device. The MIN differs from the electronic serial number, which is the unit number assigned by a phone manufacturer. MINs and ESNs may be electronically checked to help prevent fraud.

MitM **Man-in-the-Middle**

A form of network attack in which the communication between two parties is unknowingly compromised by an entity in the middle of the communication channel. This attack can act as a means of passively gathering information or actively manipulating the information sent to one or both parties. Anti-theft solutions that are improperly designed or implemented may be vulnerable to this form of attack.

MNO **Mobile Network Operator**

Mobile Device-based Anti-Theft Tool A technical solution providing anti-theft measures that execute on a mobile device, such as a smartphone, enforcing local restrictions to Essential Features. Device-based solutions use software, hardware, and cloud-based services to provide restrictions beyond what are possible with Cellular Network-based solutions. An authorized user can control the device-based solution by authenticating with credentials associated with it during initial setup.

For network based anti-theft tool, see “Cellular Network-based Anti-Theft Solution”.

MSISDN **Mobile Station Integrated Services Digital Network**

MTPD **Metro Transit Police Department**

NAFFSG **North American Fraud Forum and Security Group**

NCIC **National Crime Information Center**

For more information: http://www.fbi.gov/about-us/cjis/ncic

OEM **Original Equipment Manufacturer**

Opt-in The consumer is provided the option to activate a smartphone anti-theft solution.

Opt-out A smartphone anti-theft solution where the anti-theft solution is activated by default. The consumer is provided the option to deactivate the anti-theft solution.

OS **Operating System**

As of October 2014, there are four primary smartphone operating system platforms. They include: Android (Open Handset Alliance); BlackBerry OS (Blackberry); iOS (Apple); and Windows Phone (Microsoft).

PD **Police Department**

PII **Personally Identifiable Information (PII)**

Information that can be used to locate or identify an individual, such as names, aliases, Social Security Numbers, biometric records, and other personal information that is linked or linkable to an individual.

PIN **Personal Identification Number**

An additional security feature for mobile devices, much like a password that can prevent unauthorized access to the device or the SIM. Enabling a PIN on the SIM of a smartphone requires the user to enter that access code each time the smartphone is turned on to enable services supported by the SIM such as mobile service provider network connectivity. However, skipping the PIN entry for the SIM still allows access to the smartphone. Enabling a smartphone PIN goes beyond restricting access to cellular service, restricting access to the Essential Features of the smartphone until the PIN is entered.

Privacy Settings Ability to determine how PII is used by applications, devices and services. Consumers should always review the privacy policy of an application, device and service so they know when and how their PII will be used.

Provider Also known as a carrier, service provider or network operator, a provider is the communications company that provides cellular network service to end user customers or other carriers. They provide their customers with network service (including air time) for smartphones.

PSA **Public Service Announcement**

Ransomware A type of malware that takes control of a smartphone and encrypts stored data with a key known only to the attacker. The attacker then requires that the user pay a ransom in order to be given the key and regain access to the data.

RFC **Request for Comment**

RMS **Records Management System**

Rooting Rooting is the process of gaining privileged control to a device, by exploiting a security bug or other method, to bypass restrictions in the operating system. Once rooted, it is possible to modify system files, run applications with administrator-level permissions, and perform other typically restricted operations. The term typically refers to Android-based mobile devices. Rooting is one aspect of jailbreaking, but jailbreaking has broader implications in removing iOS-specific restrictions from devices.

SIM Card **Subscriber Identity Module Card**

A universal integrated circuit card that contains a mobile telecommunications service subscription, and the credentials pertaining to the subscriber, that fits inside some wireless devices. The SIM card communicates with a mobile wireless network via the mobile device, to authenticate the subscribers to the network and to generate encryption keys. A SIM card is entirely portable and independent of the mobile device so it may be removed and transferred to another mobile device.

Smartphone A mobile device that performs the functions of a feature phone plus is able to perform many of the functions of a computer. A smartphone typically have a relatively large screen and an operating system capable of running general-purpose applications. Unlike feature phones, smartphones have strong support for third-party applications, additional types of connectivity (Wi-Fi, Bluetooth, NFC, etc.) and more sensors (GPS, motion, advanced cameras, etc.)

SMS **Short Message Service**

Smartphone Anti-Theft Solution Another term for Mobile Device-based Anti-Theft Solution, scoped explicitly to smartphones (see "Mobile Device-based Anti-Theft Solution").

Spyware A type of malware that typically functions without a user's knowledge or permission and is designed to compromise user privacy. Spyware frequently captures user activity and sensitive data, either storing it in obscure file locations or sending it to another location on the Internet.

SSL **Secure Socket Layer**

TAC **Technological Advisory Council**

TMDA **Time Division Multiple Access**

Trader An entity either individual or corporate purchases used mobile devices with the intent to resell or to loan money against. Examples would be retailers offering 'buyback' and 'trade-in' programs as most network operators do, pawn shops, online sites offering cash for phones.

UCR **Uniform Crime Reporting**

Viruses A computer virus is a malicious program that can infect system files and is capable of replicating and transmitting itself from one source (e.g., smartphone, tablet, and computer) to another.

VPN **Virtual Private Networks**

A VPN allows a user to conduct secure communications between end points. These communications may be carried over a public or an unsecure network. By encrypting messages sent between the end points, the integrity and confidentially of the transmitted data is maintained and kept private.

Appendix B: Minnesota State Law

FAQ on Compliance requirements for Minnesota Statutes 325E.319 and 325F.698 *on Trade Practices*

(as enacted by Minnesota Bill 1740, Corrected by HF3302, Approved by the Governor on May 14, 2014.)

1. What are the requirements of the Law?

    1.1. Any smartphone sold in Minnesota must include a technical anti-theft solution (“Technical Solution”).

        1.1.1. “Smart phone" means a cellular phone or other mobile device that:

            1.1.1.1. is built on a smart phone mobile operating system;

            1.1.1.2. possesses advanced computing capability;

            1.1.1.3. enables network connectivity; and

            1.1.1.4. is capable of operating on a long-term evolution network and successor wireless data network communication standards.

            1.1.1.5. Capabilities a smart phone may possess include, but are not limited to, built-in applications, Internet access, digital voice service, text messaging, e-mail, and Web browsing.

            1.1.1.6. Smart phone does not include a phone commonly referred to as a feature or messaging phone, a laptop computer, a tablet device, or a device that has only electronic reading capability.

    1.2. Technical solution must be preloaded on the device or be downloaded on the device.

    1.3. Technical solution technical requirements are not specified. A report is due on January 15, 2015 describing anti-theft functionality principle functions of a baseline anti-theft tool that manufacturers and operating system providers will utilize on new models of smartphones in order to comply with section 1, and must describe the technology or functions included to ensure the baseline anti-theft tool is easily operable by individuals with disabilities.

2. Are manufacturers/OS providers mandated to use a particular solution?

    2.1. No, any solution that meets the requirements can be offered by a manufacturer/OS provider.

3. Are Tablets subject to compliance with the Law?

    3.1. Tablets are not subject to compliance with the law.

4. Who must supply the technical solution?

    4.1. Any entity can supply the technical solution.

5. When are smartphones required to comply with the Law?

    5.1. Any new smartphone that is manufactured on or after July 1, 2015, and sold in Minnesota after that date, shall include a technological solution.

6. What are the penalties for violation of the Law?

    6.1. No specific penalties are described by the Law.

7. If the technical solution fails (due to hacking or other third-party circumvention), is this considered a violation of the law?

    7.1. This is not considered by the law.

SF 1740 on Minnesota Statutes 325E.319 and 325F.698 on Trade Practices

Requiring any new smart phone sold or purchased in the state to be equipped with preloaded antitheft functionality (kill switch) or be capable of downloading that functionality at no cost.

[as enacted by Minnesota Bill 1740, Corrected by HF3302, Approved by the Governor on May 14, 2014]

A bill for an act

relating to telecommunications; consumer protection; requiring antitheft functionality for smart phones to deter theft; establishing requirements for acquisition and resale of wireless communications devices; proposing coding for new law in Minnesota Statutes, chapters 325E; 325F

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

ARTICLE 1

SMART PHONE ANTITHEFT PROTECTION

Section 1. **[325F.698] SMART PHONE ANTITHEFT PROTECTION**.

Subdivision 1. Definitions. (a) For the purposes of this section, the following terms have the meanings given them

(b) "Smart phone" means a cellular phone or other mobile device that: (1) is built on a smart phone mobile operating system; (2) possesses advanced computing capability; (3) enables network connectivity; and (4) is capable of operating on a long-term evolution network and successor wireless data network communication standards. Capabilities a smart phone may possess include, but are not limited to, built-in applications, Internet access, digital voice service, text messaging, e-mail, and Web browsing. Smart phone does not include a phone commonly referred to as a feature or messaging phone, a laptop computer, a tablet device, or a device that has only electronic reading capability

Subd. 2. **Antitheft functionality required**. Any new smart phone manufactured on or after July 1, 2015, sold or purchased in Minnesota must be equipped with preloaded antitheft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost.

EFFECTIVE DATE. This section is effective July 1, 2015.

Sec. 2. **REPORT ON SMART PHONE ANTITHEFT FUNCTIONALITY.**

Wireless telecommunications equipment manufacturers, operating systems providers, and wireless telecommunications service providers must either individually or jointly, by January 15, 2015, submit a report to the chairs and ranking minority members of the legislative committees with primary jurisdiction over telecommunication issues. The report must describe the principle functions of a baseline antitheft tool that manufacturers and operating system providers will utilize on new models of smart phones in order to comply with section 1, and must describe the technology or functions included to ensure the baseline antitheft tool is easily operable by individuals with disabilities

ARTICLE 2

RESALE OF CELLPHONES

Section 1. **[325E.319] WIRELESS COMMUNICATIONS DEVICES**; **ACQUISITION FOR RESALE**.

Subdivision 1. Definitions. (a) For the purposes of this section, the following terms have the meanings given them.

(b) "CMRS provider" means a provider of commercial radio service, as defined in United States Code, title 47, section 332, and includes its authorized dealers.

(c) "Internet marketplace" or "online platform" means a digitally accessible platform that facilitates commercial transactions between buyers and community-rated sellers where the operator or the platform does not take possession of, or title to, the goods bought or sold.

(d) "Law enforcement agency" or "agency" means a duly authorized municipal, county, campus, transit, park, state, or federal law enforcement agency.

(e) "Repair and refurbishment program" means a program, offered by a CMRS provider, manufacturer, or retailer who is not primarily engaged in purchasing personal property of any type from a person who is not a wholesaler, through which used or previously owned wireless communications devices are restored to good working order.

(f) "Trade-in program" means a program offered by a CMRS provider, manufacturer, or retailer who is not primarily engaged in purchasing personal property of any type from a person who is not a wholesaler, pursuant to which used wireless communications devices are accepted from customers in exchange for either (1) a noncash credit usable only for the purchase of goods or services from the CMRS provider, manufacturer, or retailer, or (2) a rebate from a manufacturer on the purchase of one of the manufacturer's wireless communications devices.

(g) "Wireless communications device dealer" or "dealer" means an individual, partnership, limited partnership, limited liability company, corporation, or other entity engaged in the business of buying or selling used wireless communications devices.

(h) "Wireless communications device" has the meaning given in section 169.011, subdivision 94.

(i) "Wireless communications device manufacturer" or "manufacturer" means an individual, partnership, limited partnership, limited liability company, corporation, or other entity engaged in the business of manufacturing wireless communications devices.

Subd. 2. **Purchase or acquisition record required**. (a) Every wireless communications device dealer, including an agent, employee, or representative of the dealer, but not an internet marketplace, shall keep a written record at the time of each purchase or acquisition of a used wireless communications device for resale. The record must include the following and may be kept in electronic form:

(1) an accurate account or description of the wireless communications device purchased or acquired;

(2) the date, time, and place or the online platform the wireless communications device was purchased or acquired;

(3) the name and address of the person selling or delivering the wireless communications device;

(4) the number of the check or electronic transfer used to purchase the wireless communications device;

(5) the number of the seller's driver's license, Minnesota identification card number, or other identification number from an identification document issued by any state, federal, or foreign government if the document includes the person's photograph, full name, birth date, and signature; and

(6) a statement signed by the seller, under penalty of perjury as provided in section 609.48, attesting that the wireless communications device is not stolen and is free of any liens or encumbrances and the seller has the right to sell it.

(b) Records required to be maintained under this subdivision shall be retained by the wireless communications device dealer for a period of three years.

(c) The record, as well as the wireless communications device purchased or received, shall at all reasonable times be available for inspection by any law enforcement agency.

(d) No record is required for wireless communications devices purchased from merchants, manufacturers, or wholesale dealers having an established place of business, but a bill of sale or other evidence of open or legitimate purchase of the wireless communications device shall be obtained and kept by the wireless communications device dealer, which must be shown upon demand to any law enforcement agency.

(e) Except as otherwise provided in this section, a wireless communications device dealer or the dealer's agent, employee, or representative may not disclose personal information received pursuant to paragraph (a) concerning a customer without the customer's consent unless the disclosure is made in response to a request from a law enforcement agency. A wireless communications device dealer must implement reasonable safeguards to protect the security of the personal information and prevent unauthorized access to or disclosure of the information. For purposes of this paragraph, "personal information" is any individually identifiable information gathered in connection with a record under paragraph (a).

Subd. 3. **Records; prohibitions**. A wireless communications device dealer, including an agent, employee, or representative of the dealer, shall not:

(1) make any false entry in the records of transactions involving a used wireless communications device;

(2) falsify, obliterate, destroy, or remove from the place of business the records, books, or accounts relating to used wireless communications device transactions;

(3) refuse to allow the appropriate law enforcement agency to inspect records or any used wireless communications device in the dealer's possession during the ordinary hours of business or other times acceptable to both parties;

(4) fail to maintain a record of each used wireless communications device transaction for three years; or

(5) purchase a used wireless communications device from a person under the age of 18 years.

Subd. 4. **Payment for used wireless communications devices**. A wireless communications device dealer shall pay for purchases of all used wireless communications devices by check mailed to a specific address or by electronic transfer.

Subd. 5. **Investigative holds; confiscation of property**. (a) Whenever a law enforcement official from any agency has probable cause to believe that a wireless communications device in the possession of a wireless communications device dealer is stolen or is evidence of a crime and notifies the dealer not to sell the item, the dealer shall not (1) process or sell the item, or (2) remove or allow its removal from the premises. This investigative hold must be confirmed in writing by the originating agency within 72 hours and will remain in effect for 30 days from the date of initial notification, until the investigative hold is canceled or renewed, or until a law enforcement notification to confiscate or directive to release is issued, whichever comes first.

(b) If a wireless communications device is identified as stolen or as evidence in a criminal case, a law enforcement official may:

(1) physically confiscate and remove the wireless communications device from the wireless communications device dealer, pursuant to a written notification;

(2) place the wireless communications device on hold or extend the hold under paragraph (a), and leave the device at the premises; or

(3) direct its release to a registered owner or owner's agent.

(c) When an item is confiscated, the law enforcement agency doing so shall provide identification upon request of the wireless communications device dealer, and shall provide the name and telephone number of the confiscating agency and investigator, and the case number related to the confiscation.

(d) A wireless communications device dealer may request seized property be returned in accordance with section 626.04.

(e) When an investigative hold or notification to confiscate is no longer necessary, the law enforcement official or designee shall notify the wireless communications device dealer.

(f) A wireless communications device dealer may sell or otherwise dispose of the wireless communications device if:

(1) a notification to confiscate is not issued during the investigative hold; or

(2) a law enforcement official does not physically remove the wireless communications device from the premises within 15 calendar days from issuance of a notification to confiscate.

(g) If a wireless communications device dealer is required to hold the wireless communications device at the direction of law enforcement for purposes of investigation or prosecution, or if the device is seized by law enforcement, the wireless communications device dealer and any other victim is entitled to seek restitution, including any out-of-pocket expenses for storage and lost profit, in any criminal case that may arise from the investigation against the individual who sold the wireless communications device to the wireless communications device dealer.

Subd. 6. **Video security cameras required**. (a) Each wireless communications device dealer shall install and maintain at each physical location video surveillance cameras, still digital cameras, or similar devices positioned to record or photograph a frontal view showing a readily identifiable image of the face of each seller of a wireless communications device who enters the physical location.

(b) The video camera or still digital camera must be kept in operating condition and must be shown upon request to a properly identified law enforcement officer for inspection.

The camera must record and display the accurate date and time. The video camera or still digital camera must be turned on at all times when the physical location is open for business and at any other time when wireless communications devices are purchased or sold.

(c) Recordings and images required by paragraph (a) shall be retained by the wireless communications device dealer for a minimum period of 30 days and shall at all reasonable times be open to the inspection of any properly identified law enforcement officer.

Subd. 7. **Criminal penalty**. A wireless communications device dealer, or the agent, employee, or representative of the wireless communications device dealer, who intentionally violates a provision of this section is guilty of a misdemeanor.

Subd. 8. **Application**. (a) This section does not apply with respect to a wireless communications device returned to the store where it was originally purchased pursuant to the return policies of the wireless communications device dealer, CMRS provider, manufacturer, or retailer.

(b) This section does not apply with respect to wireless communications devices acquired by a: (1) CMRS provider as part of a trade-in program; (2) manufacturer as part of a trade-in program or a repair and refurbishment; or (3) retailer whose trade-in program: (i) reports records to the Minnesota Automated Property System in an interchange file specification format maintained by the system; (ii) reports to other national or regional transaction reporting database available to law enforcement; or (iii) reports as required by local ordinance.

(c) This section does not apply to wireless communications device dealers regulated under chapter 325J.

EFFECTIVE DATE. This section is effective July 1, 2014.

Appendix C: California State Law

FAQ on Compliance requirements for California Section 22761 of the Business and Professions Code

(as enacted by California Bill 962, Approved by the Governor on August 25, 2014.)

1. What are the requirements of the Law?

   1.1. Any smartphone sold in California must include a technical anti-theft solution ("Technical Solution").

      1.1.1. "Smartphone" means a cellular radio telephone or other mobile voice communications handset device that includes all of the following features:

         1.1.1.1. Utilizes a mobile operating system.

         1.1.1.2. 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.

         1.1.1.3. Has wireless network connectivity.

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

      1.1.2. "Smartphone" does not include a radio cellular telephone commonly referred to as a "feature" or "messaging" telephone, a laptop, a tablet device, or a device that only has electronic reading capability.

   1.2. Technical solution must be provided at the time of sale.

   1.3. Technical solution once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user.

      1.3.1. "Essential features" of a smartphone are 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 applications.

      1.3.2. "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 predesignated by the owner.

   1.4. The smartphone shall, during the initial device setup process, prompt an authorized user to enable the technological solution.

   1.5. The technological solution shall 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.

   1.6. A technological solution may consist of software, hardware, or a combination of both software and hardware.

1.7. Technical solution shall be able to withstand a hard reset or operating system downgrade and shall prevent reactivation of the smartphone on a wireless network except by an authorized user.

1.7.1. "Hard reset" means 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.

2. Are manufacturers/OS providers mandated to use a particular solution?

2.1. No, any solution that meets the requirements can be offered by a manufacturer/OS provider.

3. Are "feature" or "messaging" telephones, laptops, tablets, or a device that only has electronic reading capability subject to compliance with the Law?

3.1. None of those devices are subject to compliance with the law.

4. Who must supply the technical solution?

4.1. The technical solution must be provided by the manufacturer or operating system provider.

5. When are smartphones required to comply with the Law?

5.1. Any smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, shall include a technological solution.

5.2. Any smartphone model that was first introduced prior to January 1, 2015, that 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, is not subject to the requirements of this law.

6. What are the penalties for violation of the Law?

6.1. The knowing retail sale of a smartphone in California in violation of the law may 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 smartphone sold in California in violation.

7. How are the penalties enforced?

7.1. A suit to enforce the penalties may only be brought by the Attorney General, a district attorney, or a city attorney.

8. Who will pay penalties?

8.1. The entity/entities named in the lawsuit.

9. If the technical solution fails (due to hacking or other third-party circumvention), is this considered a violation of the law?

9.1. A failure of the technological solution due to hacking or other third-party circumvention may be considered a violation, only 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

Senate Bill No. 962

CHAPTER 275

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

[Approved by Governor August 25, 2014. Filed with Secretary of State August 25, 2014.]

LEGISLATIVE COUNSEL'S DIGEST

SB 962, Leno. Smartphones.

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

This bill would require that any smartphone, as defined, that is manufactured on or after July 1, 2015, and sold in California after that date, include a technological solution at the time of sale, which may consist of software, hardware, or both software and hardware, that, once initiated and successfully communicated to the smartphone, can render inoperable the essential features, as defined, of the smartphone to an unauthorized user when the smartphone is not in the possession of an authorized user. The bill would require that the technological solution, when enabled, be able to withstand a hard reset, as defined, and prevent reactivation of the smartphone on a wireless network except by an authorized user. The bill would make these requirements inapplicable when the smartphone is resold in California on the secondhand market or is consigned and held as collateral on a loan. The bill would additionally except from these requirements a smartphone model that was first introduced prior to January 1, 2015, that 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. The bill would authorize an authorized user to affirmatively elect to disable or opt-out of the technological solution at any time. The bill would make the knowing retail sale in violation of the bill’s requirements subject to a civil penalty of not less than $500, nor more than $2,500, for each violation. The bill would limit an enforcement action to collect the civil penalty to being brought by the Attorney General, a district attorney, or city attorney, and would prohibit any private right of action to collect the civil penalty.

The bill would prohibit any city, county, or city and county from imposing requirements on manufacturers, operating system providers, wireless carriers, or retailers relating to technological solutions for smartphones.

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

SECTION 1. The Legislature finds and declares all of the following:

(a) According to the Federal Communications Commission, smartphone thefts now account for 30 to 40 percent of robberies in many major cities across 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) In order to be effective, antitheft technological solutions need to be ubiquitous, as thieves cannot distinguish between those smartphones that have the solutions enabled and those that do not. As a result, the technological solution should be able to withstand a hard reset or operating system downgrade, come preequipped, and the default setting of the solution shall be to prompt the consumer to enable the solution during the initial device setup. Consumers should have the option to affirmatively elect to disable this protection, but it must be clear to the consumer that the function the consumer is electing to disable is intended to prevent the unauthorized use of the device.

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) (A) “Smartphone” means a cellular radio telephone or other mobile voice communications handset device that includes all of the following features:

(i) Utilizes a mobile operating system.

(ii) 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.

(iii) Has wireless network connectivity.

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

(B) A “smartphone” does not include a radio cellular telephone commonly referred to as a “feature” or “messaging” telephone, a laptop, a tablet device, or a device that only has electronic reading capability.

(2) “Essential features” of a smartphone are 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 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 predesignated by the owner.

(3) “Hard reset” means 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.

(4) “Sold in California,” or any variation thereof, means 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.

(b) (1) Except as provided in paragraph (3), any smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, shall 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 of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user. The smartphone shall, during the initial device setup process, prompt an authorized user to enable the technological solution. The technological solution shall 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. A technological solution may consist of software, hardware, or a combination of both software and hardware, and when enabled, shall be able to withstand a hard reset or operating system downgrade and shall prevent reactivation of the smartphone on a wireless network except by an authorized user.

(2) An authorized user of a smartphone may affirmatively elect to disable or opt-out of enabling the technological solution at any time. However, 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.

(3) Any smartphone model that was first introduced prior to January 1, 2015, that 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, is not subject to the requirements of this section.

(c) The knowing retail sale of a smartphone in California in violation of subdivision (b) may 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 smartphone sold in California in violation of this section. A suit to enforce this subdivision may only be brought by the Attorney General, a district attorney, or a city attorney. A failure of the technological solution due to hacking or other third-party circumvention may be considered a violation for purposes of this subdivision, only 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. There is no private right of action to enforce this subdivision.

(d) The retail sale in California of a smartphone shall not result in any civil liability to the seller and its employees and agents from that retail sale alone if the liability results from or is caused by failure of a technological solution required pursuant to this section, including any hacking or other third-party circumvention of the technological solution, 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. Nothing in this subdivision precludes 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.

(e) Any request by a government agency to interrupt communications service utilizing a technological solution required by this section is subject to Section 7908 of the Public Utilities Code.

(f) Nothing in this section prohibits 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 pursuant subdivision (b).

(g) Nothing in this section requires 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:

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

(2) Participation in the wireless emergency alert system.

(3) Participation in state and local emergency alert and public safety warning systems.

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

Appendix D: Detailed Information for Existing Solutions

The following subsections of this Appendix provide detailed information for existing solutions and are grouped into the following categories:

- Database Solutions.
- Device Based Solutions.
- Third Party Solutions.
- Wireless Operator Implementations.

D.1 Database Solutions

There are various existing database solutions available to address the problem of the mobile device theft. The following database solutions are described in this section:

- Device Blocking
- GSMA IMEI Database
- iconectiv
- Insurance Databases
- Recipero
- Subscriber Registry

The descriptions for each of the database solutions cover the following topics:

- Non-Technical Description, Capabilities & Functions
- Connectivity Requirement
- Constraints or Dependencies
- Impact to Flow
- Level of Accessibility and Funding Model
- Status of Availability
- Reference URL

D.1.1 Device Blocking

Device blocking is a solution defined in global standards. The solution for GSM, UMTS, and LTE uses the GSMA IMEI Database available from the GSM Association (GSMA) along with solutions in wireless operator networks. An example of the LTE network implementation to support device blocking appears below:

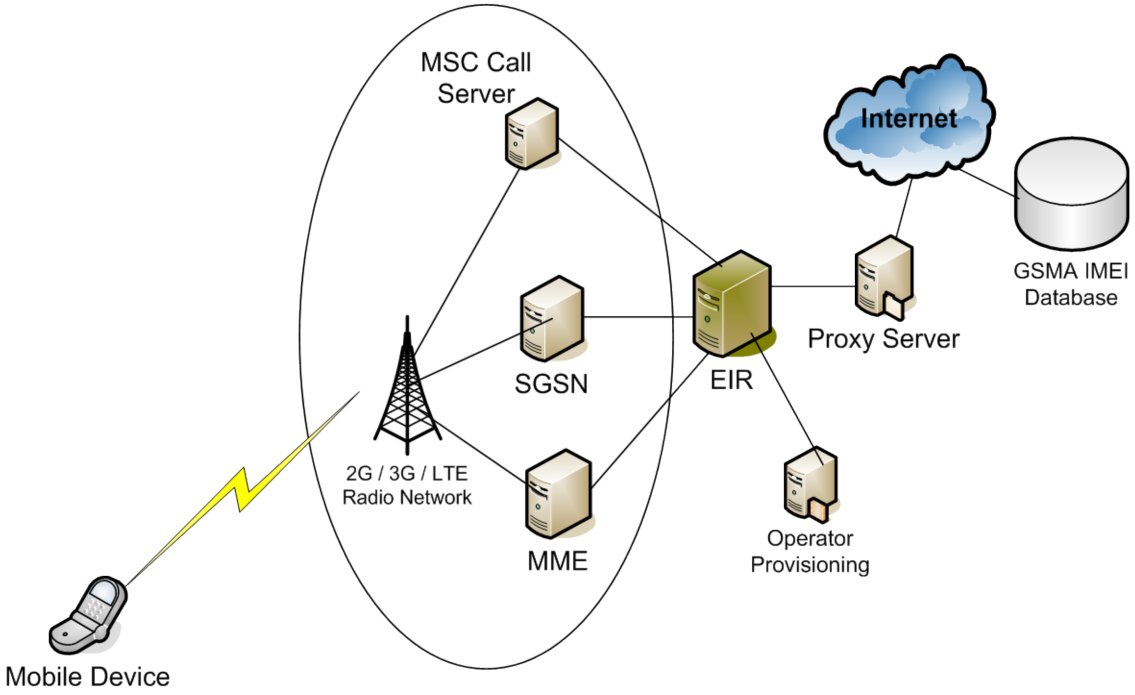


Figure 11: Example Device Blocking Implementation

A call flow for an LTE network, described in standards, of how a device check is made on an operator network is as follows:

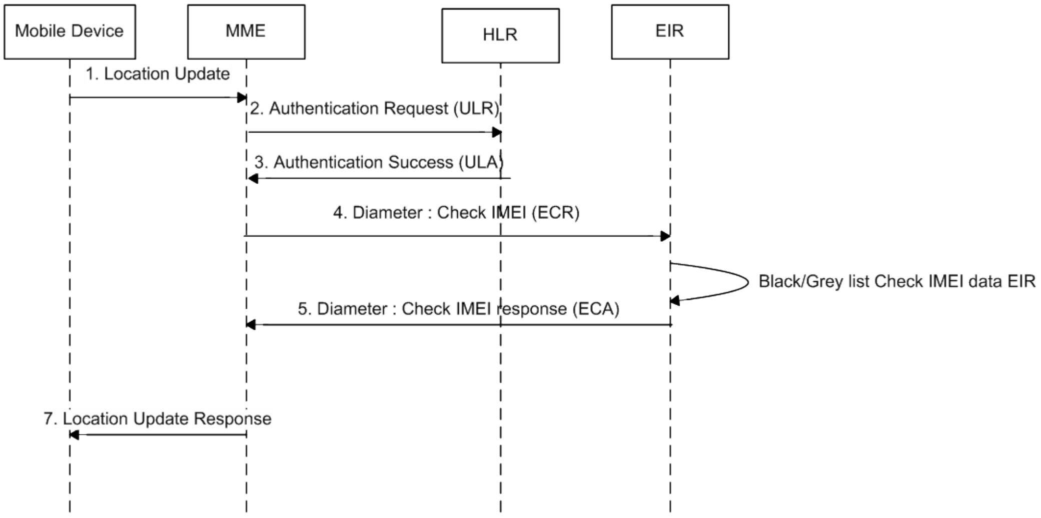

Mobile Device
MME
HLR
EIR
1. Location Update
2. Authentication Request (ULR)
3. Authentication Success (ULA)
4. Diameter : Check IMEI (ECR)
Black/Grey list Check IMEI data EIR
5. Diameter : Check IMEI response (ECA)
7. Location Update Response

Figure 12: Device Blocking Call Flow for LTE Network

Non-Technical Description, Capabilities & Functions

- Every mobile device has a unique identifier (IMEI) that is allocated to handset manufacturers by GSMA.
- Carriers maintain a blacklist of IMEIs, within their Equipment Identity Register, that must be denied network access.
- The IMEI is transmitted to the mobile network when the device attempts access on the network.
- Carriers check the IMEI received from the device attempting access against the blacklist and any matching IMEI is denied network access.

Connectivity Requirement

- Manufacturers obtain their IMEIs via a dedicated secure website maintained by GSMA.
- Mobile devices transmit their IMEIs over the mobile radio network to be checked within the core network.
- Provisioning systems are needed to allow operator staff to place stolen device IMEIs in the network's blacklist.

Constraints or Dependencies

- IMEI blocking can be undermined and bypassed if the device identifiers are changed.
- IMEIs only apply to GSM, UMTS and LTE devices and on networks that support those technologies – devices may use other access technologies and services.

Impact to Flow

- IMEI allocation is what allows each device to be uniquely identified and blocked but this doesn't impact.
- The placement of the IMEI on the EIR blacklist by the carriers is what gives effect to device blocking.
- Processes need to be developed to allow the operators to identify and verify IMEIs to be blacklisted.

Level of Accessibility and Funding Model

- IMEI allocations for placement in devices are available from GSMA to all legitimate device manufacturers.
- Operators must deploy EIRs for device blocking to work and these are significantly expensive to deploy and to integrate with other essential provisioning systems.

Status of Availability

Available since the inception of GSM but not every operator has invited in or deployed an EIR.

Reference URL

http://www.gsma.com/technicalprojects/fraud-security/device-imei.

D.1.2 GSMA IMEI Database

The solution available from the GSM Association (GSMA) is called the "IMEI Database". This solution is the recommended solution that has been implemented by North American GSM and LTE operators, as described in the GSMA-NA "Analysis and Recommendations for Stolen Mobile Device Issue in the United States".

The GSMA maintains a unique system known as the IMEI Database, which is a global central database containing basic information on serial number (IMEI) ranges of millions of mobile devices (e.g., mobile phones, laptop data cards, etc.) that are in use across the world's mobile networks.

The IMEI must be unique for each device, so there needs to be a way of managing allocations of IMEIs to handset manufacturers to ensure that no two devices use the same IMEI. The GSM Association performs this role, and records all of the IMEIs that are allocated to mobile device manufacturers in the IMEI Database. When reserving IMEIs for a device manufacturer, the GSMA stores some basic information associated with the IMEI. This information includes the manufacturer name and the model identifier of the associated handset and some of its technical capabilities (e.g., frequency bands supported by the handset, the handset power class, etc.).

The GSMA provides access to the IMEI Database to its members, the mobile network operators across the world, and to qualified industry parties (i.e., manufacturers of device management products). The network operators use the information in the IMEI Database to determine what types of devices are being used by their customers, and what features they support, so that they can offer and support the latest services to these customers through their networks.

The IMEI Database also supports what is known as a "black list". The black list is a list of IMEIs that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. Previously known as the Central Equipment Identify Register (CEIR), the IMEI Database acts as a central system for network operators to share their individual black lists so that devices denied service (blacklisted) by one network will not work on other networks even if the SIM card in the device is changed.

Network operators who deploy Equipment Identity Registers (EIR) in their networks use them to keep their own lists of blacklisted lost or stolen phones. Operators' EIRs automatically connect to the IMEI Database to share their latest lists of blacklisted devices with other operators. The IMEI Database takes the black lists from the various operators around the world that are connected to system and it compiles the data into one global black list. When a network operator EIR subsequently connects to the IMEI Database, it downloads the latest global black list (or a national or regional subset of the global list) for its own use. By loading the IMEI Database black list onto the local EIR, all handsets reported as stolen on other connected networks up to the previous day are now also capable of being blocked on that network.

As GSM, 3G, and LTE devices have become more sophisticated and more expensive, they are also unfortunately more attractive to thieves. Recent years have seen an increased need for the IMEI Database to be used as a tool to combat handset theft. Many mobile network operators have responded to the problem of handset theft by deploying EIRs in their networks and connecting them to the IMEI Database. The engagement of governments and law enforcement agencies with the network operator community continues in a number of markets where handset theft is perceived to be a problem and the GSM Association strongly encourages use of the IMEI Database as a platform to exchange stolen handset data and it welcomes all of its members to connect to the system.

Non-Technical Description, Capabilities & Functions

- Central repository of identifiers allocated to device manufacturers by GSMA for use in mobile devices.
- Receives device identifiers from carriers pertaining to devices reported stolen by their customers.
- Stolen handset data received is collated and securely distributed to other carriers connected to the database.
- Data downloaded from IMEI Database is loaded in carrier's EIR to deny network access to lost/stolen devices.
- Checking service available to authorized dealers, repair centers, insurers, recyclers, regulators and law enforcement.

Connectivity Requirement

- Secure FTP by carrier users to upload and download data.
- Web site & API by eligible third parties, such as law enforcement, insurers, recyclers, etc. that wish to check IMEIs.

Constraints or Dependencies

- IMEIs only apply to GSM and LTE devices. CDMA devices use different format identifiers from IMEIs that are not currently sent to GSMA blocking database. However the capability is in place to accept these.
- Value depends on the number of carriers connected and the extent to which data is shared – gaps exist in USA.

Impact to Flow

- Primary method of denying network access to stolen devices.
- Mature technology based on open standards and well established principles.
- Critical component to support device blocking, data sharing and distribution and device status checking.

Level of Accessibility and Funding Model

- Available to carriers and law enforcement agencies at no cost.
- Fees apply, on a cost recovery basis, to commercial stakeholders that choose to check IMEIs.

Status of Availability

- Available since 1996 to carriers.
- Access extended in 2005 to eligible 3rd party stakeholders, including LEAs.

Reference URL

http://www.gsma.com/technicalprojects/fraud-security/imei-database.

D.1.3 iconectiv

The iconectiv Device Registry is a comprehensive centralized device analytics solution that automatically discovers mobile device data from multiple sources including Operator networks to provide powerful insights regarding mobile devices. By consolidating real-time and non-real time data collection of mobile data in a common context, Device Registry product can address both traditional mobile equipment challenges, such as anti-theft, invalid device blocking and cloning detection, and also provide lifecycle analysis of mobile devices and subscribers over multiple data pivot points—such as IMEI, IMSI, MSISDN—while providing a valuable source of information for manufacturers, Operators, national regulators, customs and taxation, law enforcement and national security organizations. It is not limited to IMEI only devices. It can analyze different device types such as Data-only Wi-Fi devices, wearables, IoT devices and even feature phones. It correlates patterns across aggregated devices and can be used to detect mobile crime as well as provide Business Intelligence. It has a SMS capability to reach subscribers to validate device status.

Non-Technical Description, Capabilities & Functions

Comprehensive device analytics solution that integrates information from multiple sources using automated discovery techniques to:

1. Detect stolen devices.
2. Detect non-compliant devices (counterfeits, clones and illegal devices, e.g., those that evade Customs). Provide powerful insights such as device trail across all networks, SIM swap detection, etc. in a timely manner. This enables actions based on aggregated inform to thwart the movement of stolen devices and also understand how and where such devices land and how they get re-used.
3. In addition, it also provides value by providing trend analysis, network Audit capabilities and Business Intelligence including types of devices on the network, device demographics based on capabilities such as NFC enabled, Bluetooth, etc.

- A key component is the Device Registry Gateway that collects data from Operator networks and filters it.
- A central database function integrates information across all sources and is used for advanced analytics.

- Results include a black list of stolen devices that can be exported to the GSMA by carriers, non-compliant devices list such as counterfeits & clones and other analytics based on policies.
- The output is provided as a dashboard with query interface and reports.
- In addition, a SMS messaging interface is provided to interact with the subscriber to validate device status and obtain additional information if required.

The solution is extendable by design and can encompass different types of devices including M2M devices and Data-only devices.

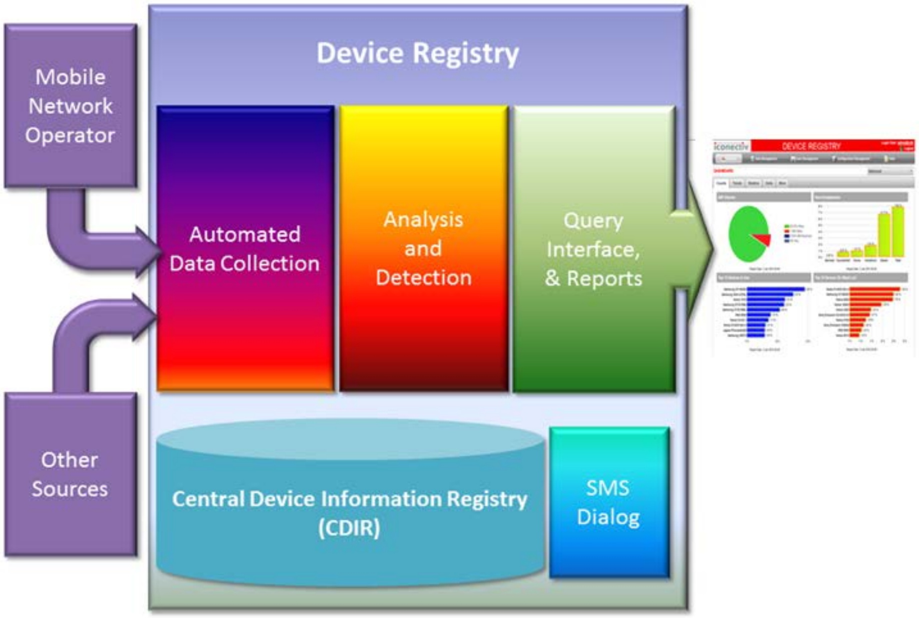


Figure 13: iconectiv Device Registry

Connectivity Requirement

- Network based solution, connectivity required between Operators and central Device Registry.
- Solution can be obtained as a Cloud based service or as an on-site managed service; for the former connectivity to the Cloud is required.

Constraints or Dependencies

- Automated collection of current device records from from different sources such as Operators networks.
- Includes blacklists as input.

- Uses the Equipment Identity Registry (EIR) to enforce blocking of devices.

Impact to Flow

- Law Enforcement/Government/Regulators/Customs, Operators and third-parties such as financial risk agencies, insurers can leverage the Device Registry to:
    a. Query for pinpointed device information including status, location, capabilities; diagnose device trail across operators and obtain other analytical insights into the network.
    b. Enforce policies such as blocking the blacklisted device from the network and tracking of counterfeits, clones, suspected stolen devices.
    c. Interact with a subscriber via SMS to validate information if required.
- Gains insights regarding blacklisted and cloned devices on the networks.

Level of Accessibility and Funding Model

- Subscription model or transaction based.
- Cloud based or on-site deployment.
- Provides query interface for pinpointed information and analysis, reports, dashboard and SMS messaging capability to reach subscribers.

Status of Availability

Yes, in market.

Reference URL

http://www.iconectiv.com/anti-theft/device-registry/index.html.

D.1.4 Recipero

The solution available from Recipero is a crime reduction eco-system with services for carriers, traders, insurers, public and police. Recipero believes that the market for stolen goods has to be closed in order to remove the incentive to steal.

Non-Technical Description, Capabilities & Functions

- Recipero's ecosystem takes in loss and theft data from the GSMA/CTIA system, CDMA carriers (outside GSMA/CTIA), Insurer claims, Finance agreements, consumer loss & theft, police reported loss & theft and a variety of other proprietary sources that influence the legal title or status of a device.
- The ecosystem provides user type specific tools (to police, insurers, carriers, retailers, the public) to allow checking of aggregated data to ensure that a lost, stolen or otherwise compromised device may be detected and an illegal trade avoided.

Connectivity Requirement

Both web interfaces and server to server Application Programming Interfaces are available.

Constraints or Dependencies

- Some data (from some notable CDMA carriers for example) and carrier activation status is not currently accessible to Recipero or other aggregators. If activation status were available it would prevent a class of thefts from being perpetrated that are not addressable by device solutions or blocking. This can directly impact 'credit muling' for example a particularly socially damaging crime.

Impact to Flow

- Use of the ecosystem to detect and prevent the trade of stolen devices has zero impact on the responsible seller, assuming they were also a responsible buyer initially.
- The ecosystem has a large number of point-of-sale integrations and as such provides extremely effective prevention of stolen device trade, impacting the incentive to steal and reducing mobile device theft.
- It impacts the flow of devices internationally as well as domestically.

Level of Accessibility and Funding Model

- All elements of Recipero’s ecosystem are readily accessible to all stakeholders.
- The ecosystem is self-funding for traders and carriers, generating massive savings in bad transaction avoidance.
- Recipero's ecosystem offers free voluntary consumer device registration to assist consumer and law enforcement agency to communicate and increase repatriation rates.
- Free for law enforcement use.

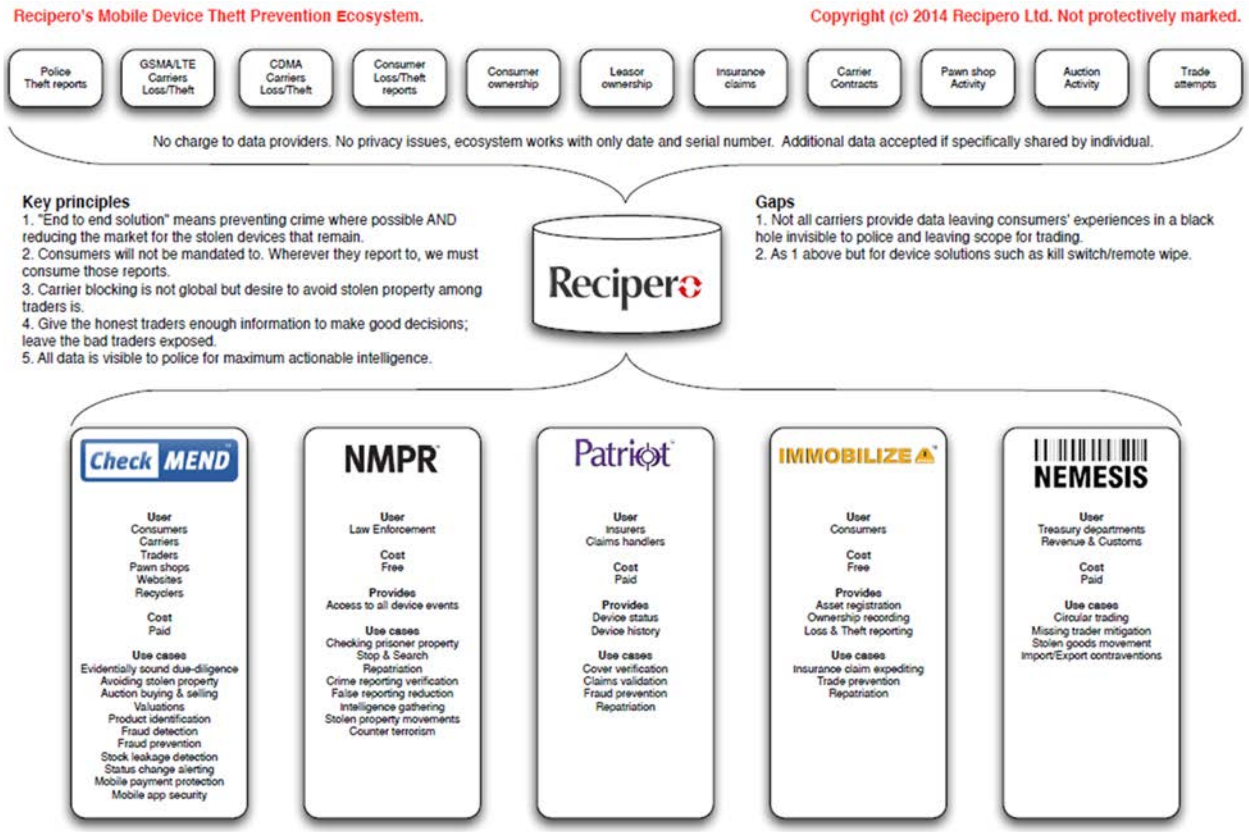
Status of Availability

- LEAs can register free of charge and obtain access quickly after simple verification.
- The ecosystem operates globally to detect US device movement internationally and to prevent trade of those devices. Equally it prevents domestic trade of devices stolen from other countries.
- Recipero’s solution has been in use by UK government and police agencies for over 10 years and is widely regarded to have played a leading role in empowering the UK recycling and recommence sector over the last 10 years. It is the only system that is compliant with the requirements of the UK’s voluntary Recyclers’ Code of Practice scheme.
- The ecosystem sits as a cornerstone of the UK’s efforts to curb mobile device theft and is already impacting US device flow with many household names using the solution.

Reference URL

www.recipero.com.

The following figure depicts the end to end solution of the Recipero Mobile Device Theft Prevention Ecosystem in the US:



Recipero's Mobile Device Theft Prevention Ecosystem.

Copyright (c) 2014 Recipero Ltd. Not protectively marked.

No charge to data providers. No privacy issues, ecosystem works with only date and serial number. Additional data accepted if specifically shared by individual.

Key principles

1. "End to end solution" means preventing crime where possible AND reducing the market for the stolen devices that remain.
2. Consumers will not be mandated to. Wherever they report to, we must consume those reports.
3. Carrier blocking is not global but desire to avoid stolen property among traders is.
4. Give the honest traders enough information to make good decisions; leave the bad traders exposed.
5. All data is visible to police for maximum actionable intelligence.

Gaps

1. Not all carriers provide data leaving consumers' experiences in a black hole invisible to police and leaving scope for trading.
2. As 1 above but for device solutions such as kill switch/remote wipe.

Figure 14: Recipero End-to-End Mobile Device Theft Prevention Solution

D.1.5 Subscriber Registry

A subscriber registry is a centralized national database of mobile subscribers in the country. It typically involves a subscriber registering their mobile device with the national registry. It maps the identity of the subscriber with the mobile device used by the subscriber. If the subscriber changes her device or changes the Operator providing cellular service, the change is reflected in the subscriber registry. This process is very similar to registration of automobile to obtain a VIN number for identification. According to the GSMA, in 2013, around 80 countries in the world have either deployed such a registry or are contemplating on doing do. Examples include Australia, UAE and Thailand. In Thailand, a mobile app has been used to register subscribers on activation of their mobile devices.

The solution typically is custom built or would leverage a solution such as the iconectiv Device Registry.

Non-Technical Description, Capabilities & Functions

- Registry of mobile subscribers with their contact information, national ID, IMEI and mobile device SIM information. Note: The information held in such device registries vary; some include SIM alone with the IMEI while others also contain identification/compliance information.
- Provides digital identity for m-commerce, Government e-services and national security.
- Similar to registering automobiles in the country (VIN card to identify autos in the US).
- In some countries they are looking to add SIMs used in their smart grid network.

Connectivity Requirement

Secure access by Government, Regulators, Customs, Law Enforcement, Operators and subscribers.

Constraints or Dependencies

- Hosted typically on-site as a managed service as data is sovereign to the country.
- Dependent on valid ID information (can be a problem when prepaid users don’t need to provide ID to obtain the device).

Impact to Flow

- Owner and device details available for use by law enforcement to close a stolen device case when device retrieved or has to be re-activated.
- Device changes are up-to-date when the device information is collected in an automated manner.

Level of Accessibility and Funding Model

Registration fee is typically collected by Government, operators and/or other stakeholders. Many of these registries also allow consumers to access it to attest the validity of their device based on device identifiers such as the IMEI.

Status of Availability

Eighty countries around the world either have implemented subscriber registries or are thinking of doing so.

Reference URL

http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf.

The following figure is Figure 1 of the GSM Association white paper on mandatory registration of prepaid SIM card users[68]:

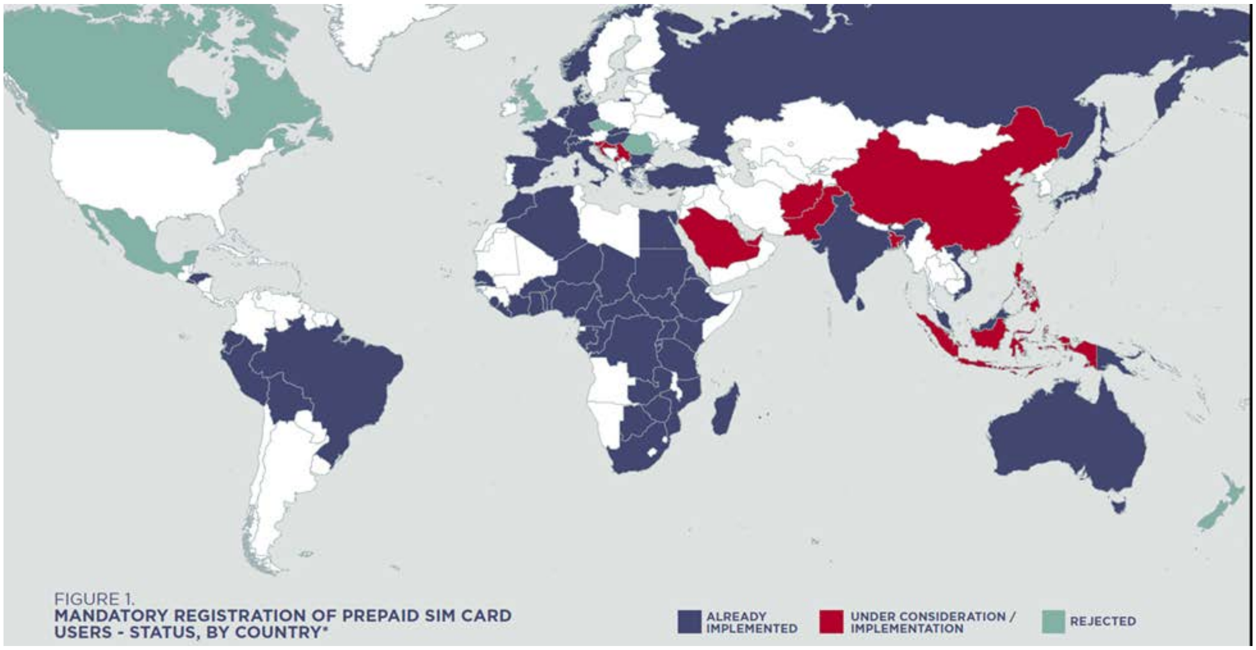


FIGURE 1.
MANDATORY REGISTRATION OF PREPAID SIM CARD USERS - STATUS, BY COUNTRY*
ALREADY IMPLEMENTED
UNDER CONSIDERATION / IMPLEMENTATION
REJECTED

Figure 15: National Subscriber Registry Efforts around the World

D.2 Device Solutions

This section describes the following existing device solutions for the prevention of the mobile device theft:

- Apple
- Blackberry
- Google
- LG
- Microsoft
- Motorola Mobility
- Qualcomm
- Samsung

The descriptions for each of the device solutions which cover the following topics:

- Non-Technical Description, Capabilities & Functions
- Connectivity Requirement
- Constraints or Dependencies

[68] GSM Association, "The Mandatory Registration of Prepaid SIM Card Users – A White Paper", November 2013. http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf.

- Impact to Flow
- Level of Accessibility and Funding Model
- Status of Availability
- Reference URL

D.2.1 Apple

Apple's Find My iPhone is built into iOS and is part of a user's iCloud account. Once a user's device is enrolled, a user can log into either iCloud.com or the Find My iPhone app to remotely locate their device, play a sound on it, put it in lost mode, or securely erase it remotely – and the device takes these actions only in response to the user's command. Find My iPhone includes Activation Lock, which is designed to prevent anyone from turning off Find My iPhone, erasing a device or reactivating it.

Non-Technical Description, Capabilities & Functions

- Find My iPhone allows for users to remotely locate their device, play a sound on it, or erase it, all in a privacy friendly manner where the device only connects to the Find My iPhone service on prompting from a user, giving the user complete control over it.
- With iOS 7, Apple introduced Activation Lock, whereby a phone enrolled in Find My iPhone cannot be reactivated following an erase/reset without the user entering their iCloud username and password. This makes Activation Lock a reversible solution that enables users to restore their device if they recover it.
- For devices that support Apple Pay, users can suspend Apple Pay by placing their device in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone. When a user erases a device using Find My iPhone, the cards on the device are placed into an unusable state.

Connectivity Requirement

- Find My iPhone works on any iOS device running iOS 5 or above. Activation Lock is supported on devices running iOS 7 and above.
- An authorized user can use Find My iPhone through either iCloud.com or the Find My iPhone app to issue a command (locate, play a sound, or erase) to a device. The device receives the command when it is connected to the Internet either over cellular or WiFi.

Constraints or Dependencies

Find My iPhone works on any iOS device running iOS 5 or above, and iCloud.com can be accessed from any modern web browser.

Impact to Flow

- With iOS 8, if a user chooses to use iCloud when setting up a new device, Find My Phone will automatically be enabled on that device.
- Activation Lock is enabled as part of enrolling an iOS device in Find My iPhone.

- When a device is enrolled in Find My iPhone, a user's Apple ID credentials are necessary to turn off Find My iPhone, erase the device, and reactivate the device. The authentication of a user's Apple ID credentials requires network connectivity.

Level of Accessibility and Funding Model

Find My iPhone works on any iOS device running iOS 5 or above. Activation Lock is supported on devices running iOS 7 and above. Find My iPhone is available to iOS users for free at no extra cost.

Status of Availability

Available now.

Reference URL

https://www.apple.com/icloud/find-my-iphone.html.

D.2.2 Blackberry

BlackBerry Protect is an integrated, OS-based solution that provides tamper-resistant theft prevention to BlackBerry 10 devices by disabling all non-essential device functionality when theft is detected (essential functionality includes recovery screen and emergency calls to 911). Theft-mode is triggered when the device holder fails the password authentication ten times or when the registered owner with BlackBerry ID credentials remotely reports the device stolen via the BlackBerry Protect website. Theft-mode triggering also automatically executes a complete device data wipe so that all consumer information is further protected (in addition to data encryption). The BlackBerry Protect website also allows registered owners to find their lost devices via location services. Recovered devices may have theft-mode deactivated either directly through the user interface recovery screen with the registered owner's BlackBerry ID credentials or via a secure "reverse logistics" field utility that supports authorized parties in service and support environments.

Non-Technical Description, Capabilities & Functions

- Device-based solution that leverages BlackBerry ID consumer credentials so that registered owners can report stolen devices, thereby blocking all functionality of devices except for device recovery screen and emergency calls. Theft-mode can also be triggered automatically on the device when the device holder fails the required password authentication for device start-up or log-on.
- BlackBerry Protect also provides other consumer remote security functionality, including locating devices via GPS and device data wiping.

Connectivity Requirement

Connectivity is not required to trigger theft-mode because device-based functionality will detect tampering associated with theft (ten failed password attempts), thereby triggering device into theft-mode; but connectivity provides an additional option to remotely report stolen devices via BlackBerry Protect consumer website. Cellular or WiFi connectivity can be used to disengage theft-mode from recovered devices (other options for disengaging theft-mode include the device recovery screen or the "reverse logistics" field service utility).

Constraints or Dependencies

Support with upcoming BlackBerry 10 release.

Impact to Flow

- User is guided through process to activate BlackBerry Protect with out-of-the-box experience (user must opt-out).
- Theft-mode is engaged if:
  - Device holder fails to authenticate to BlackBerry device either on device startup and/or on device log-on/password unlock (restarting device does not circumvent theft-mode, and device cannot be reset to "factory settings" once theft-mode is activated).
  - Device is remotely reported as stolen via registered owner with BlackBerry ID credentials visiting the BlackBerry Protect website.
- Engagement of theft-mode will also automatically execute a complete device data wipe.
- If applicable, corporate owners can override theft-mode through the BlackBerry Enterprise Service.
- Authorized third parties may recover devices (disengage theft-mode) through authorized and authenticated "reverse logistics" field service utility.

Level of Accessibility and Funding Model

BlackBerry Protect with theft prevention service included with device purchase.

Status of Availability

Available for California requirements deadline.

Reference URL

Not currently available.

D.2.3 Google

The current in-market solution available from Google is called “Android Device Manager”.

Non-Technical Description, Capabilities & Functions

- Current release version (Android 2.2 and newer) allows user to remotely locate, lock, and erase an Android phone or tablet from the Device Manager App or web interface over a wireless Internet data connection. Below is a subset of the current features:
  - Users can remotely ring devices at maximum volume so user can find it (even if it’s been silenced).

  - Users can remotely reset the device password.
  - Users can remotely factory reset the device.
  - Users can locate the device on graphical map in real time.
  - Users can add a dial-back number on the locked device, so that they can be reached if a lost phone is found.
  - Users can connect as many compatible Android devices as desired to Android Device Manager.
  - Administrators and users can remotely wipe a lost or stolen device through the Google Apps Admin Console, for mobile devices that are synced to that organization's Google Apps account (applicable to Google Apps for Work, Education, Nonprofits, etc.)
- Note: In addition, Android Device Manager, devices running Android 4.4 or earlier also have device encryption available as an option and it is enabled by default in Android 5.0. By default, encrypted Android devices require a user to enter a PIN or password that is required whenever the device is booted up or attempted to be wiped.

Connectivity Requirement

Combination Device/Network based solution.

Constraints or Dependencies

- Works only on Android 2.2 and above.
- Device must be on and connected to internet for full suite of functionality to be available.

Impact to Flow

Primary Audience is End-User / "User App".

  - Android 2.3 - 4.4: Users can opt-in to Android Device Manager (ADM) on their mobile devices. ADM is automatically made available on all Android devices with Google Play through the "Google Settings" app and can also be downloaded and installed separately from Google Play.
  - Android 5.0: Android Device Manager is activated by default when a user first signs into his or her Google account on the device, either during the initial setup of the device or when upgrading a phone to Android 5.0.

Level of Accessibility and Funding Model

Free.

Status of Availability

In-Market.

Reference URL

- https://support.google.com/accounts/answer/3265955?hl=en.
- https://support.google.com/nexus/answer/4596836?hl=en-GB.

- https://support.google.com/accounts/answer/3265955?hl=en.
- http://googleblog.blogspot.com/2013/08/dude-wheres-my-phone-simple-steps-to.html.
- https://support.google.com/a/answer/173390?hl=en Google Apps.

Administrators and users can remotely wipe a lost or stolen device through the Google Apps Admin Console, for mobile devices that are synced to that organization's Google Apps account (applicable to Google Apps for Work, Education, Nonprofits, etc.).

D.2.4 LG

The solution available from LG is called "LG Anti-Theft Solution" and uses McAfee. It is based on Android OS and can be remotely operated to impose restrictions or trigger functions to protect data through wiping out, backing up and restoring, draw attention, or determine the current location of the smartphone as long as there is internet connectivity, via a cellular network or Wi-Fi. In addition, manipulation of the smart phone through factory-reset and USB connections are also blocked when the device is remotely locked. Key characteristics and descriptions of the solution are summarized as:

Non-Technical Description, Capabilities & Functions

- User can locate and track the device, lock it or wipe the data out using the service website.
- User can backup and restore data using the application and the web service.
- Factory-reset and USB connection are also blocked when the device is remotely locked.

Connectivity Requirement

Network based solution (Internet connection required via data networks including Wi-Fi).

Constraints or Dependencies

Works only with Android OS, and must have internet connection to invoke the service.

Impact to Flow

User will be asked to enroll the service during the initial device setup using Setup Agent.

- User can choose not to enroll (opt-out). User can enroll the service later when he/she wants.
- User creates an account and provides some information (email, password, etc.)
- After a PIN code is set up and the phone number is verified, the service is activated.
- Then user can track, lock and wipe the phone from the website.

Level of Accessibility and Funding Model

Available on all Android smart phones shipping after July 1, 2015. No fee for end users (customers).

Status of Availability

- In-market Q1 2015 timeframe.
- Upgrades to substantial subset of existing devices possible (TBD).

Reference URL

http://lge.mcafeemobilesecurity.com.

D.2.5 Microsoft

Microsoft provides Find My Phone as a free service on all Windows Phone OS-based smartphones. To use the feature, users sign in to a secure web portal using their Microsoft account credentials tied to the smartphone; once authenticated, users can request the smartphone's current location, cause it to ring, lock it and leave a custom message, or erase user data on it to protect personal information. Network connectivity — cellular, cellular data, or Wi-Fi — is required to deliver commands to the smartphone. A unique, secure, proprietary hardware identifier is used to link a smartphone to an account and target commands to it.

By July 2015, Find My Phone will offer additional functionality to prevent a non-owner from using the smartphone after reset or reflash to further reduce the value of a stolen Windows Phone. These changes will meet Microsoft's commitment to the CTIA Smartphone Anti-Theft Voluntary Commitment and recent legislation for "kill switch" mechanisms in smartphones.

Non-Technical Description, Capabilities & Functions

- Built-in to every Windows Phone, Find My Phone provides remote Locate, Ring, Lock, Message, and Erase capabilities.
- Locate and Ring help find and discover a lost or stolen device.
- Lock prevents access to customer information on the device until it can be recovered or reset.
- Message is an optional part of Lock to display a message on the screen (e.g., a number to call or address to email).
- Erase reformats user information to protect privacy of personal data.
- As long as there is connectivity, users are always able to perform a remote action – there is no on/off switch, but users must expressly request an action by logging into a website with their Microsoft account.
- Users can choose to periodically report location automatically so a last known location is always available.

Connectivity Requirement

- OS-level hardware, software, and service solution shipped with every device.
- Uses SMS or data (cellular data or Wi-Fi) to trigger remote commands.

Constraints or Dependencies

- Works with Windows Phone 7, 8, and 8.1 devices.

- Requires a Microsoft account to be associated with the Windows Phone.
- Requires network connectivity (cellular, cellular data, or Wi-Fi) to deliver commands.
- Utilizes a custom, secure, and persistent unique identifier built into the device hardware.
- Does not persist locked state across device reset / reflash (will be resolved to align with CTIA commitment).

Impact to Flow

- Designed for consumers and protected by their private credentials.
- Always available to users as long as there is a connection – no on/off switch.
- Users go to www.windowsphone.com/find and authenticate with their Microsoft account (that is associated with the phone) to trigger remote commands.
- An opt-in is required for automatic, periodic location reporting (but requesting a location is always possible).

Level of Accessibility and Funding Model

- Built into every Windows Phone device since October 21st, 2010.
- Available to all users for free as long as they connect a free Microsoft account to the device.
- Previously available on Windows Mobile 6.0+ as an app since February 16th, 2009 (*discontinued October 6th, 2011*).

Status of Availability

- Actively maintained and developed by Microsoft.
- Most recent software update shipped to customers in May 2014 as part of Windows Phone 8.1.
- Ongoing backend and website updates ship regularly without requiring any user action.
- Publicly committed to support CTIA commitment with an update before July 2015 for all Windows Phone 8 users.

Reference URL

- Find My Phone for users (*login required*): http://www.windowsphone.com/find.
- Find My Phone support info: http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/find-a-lost-phone.

D.2.6 Motorola Mobility

The existing solution available from Motorola Mobility's Moto Care service allows users to remotely lock, wipe, locate and ring the device from a web portal. All current models of Motorola smartphones sold in the U.S. also come pre-equipped with Android Device Manager, which provides the functionality as described in Section D.2.3.

Covered Motorola smartphones sold in the U.S. will include additional anti-theft functionality by July 1, 2015 to meet CTIA's Anti-Theft Voluntary Commitment[69], of which Motorola Mobility is a signatory, and recently enacted State requirements.

Non-Technical Description, Capabilities & Functions

- Moto Care allows user to remotely, with Internet connectivity, lock device screen to prevent unauthorized access to the device and user data.
- User can erase all user data on the device.
- User can locate device on graphical map, in real time.
- User can post a message on screen (e.g., to provide contact information for return).
- User can remotely ring device at maximum volume so user can find it (even if it's been silenced).

Connectivity Requirement

Combination Device/Network based solution.

Constraints or Dependencies

- Works on all current models of smartphones sold in the U.S., including Moto X, G, E, Droid Ultra, Droid Maxx, and Droid Turbo.
- Does not currently include anti-theft protection from unauthorized factory reset or re-flash, but upcoming functionality on covered devices will include such protection by July 1, 2015.
- Existing solution requires device to be on and connected to Internet.
- Factory reset and re-flash protections will not require connectivity, only user credentials, though restoring device would require Internet connection.
- User must opt in and have a Google account to ensure privacy and security.

Impact to Flow

Primary Audience is End-User / "User App".

- Once opted in on device, users visit Lost Device Web Portal and authenticate with a Google account to locate, lock, wipe, ring or restore device.

Level of Accessibility and Funding Model

Current and upcoming solutions are free to customer.

Status of Availability

- Moto Care and Android Device Manager in-market with devices listed above.
- Additional factory reset and re-flash protections available by July 1, 2015.

[69] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

Reference URL

https://motorola-global-portal.custhelp.com/app/answers/detail/a_id/95507.

D.2.7 Qualcomm

With Qualcomm® SafeSwitch™ technology, SafeSwitch-enabled devices can be remotely locked at a very deep level if they are lost or stolen. SafeSwitch commands are processed and authenticated by hardware, making potential attacks, such as malicious locking of phones and unlocking stolen phones, far less feasible.

SafeSwitch™ works in full harmony with Lookout Mobile Security, and can be integrated to other solutions as requested by the operator.

Non-Technical Description, Capabilities & Functions

- Users can locate, track, wipe, ring, message, or lock their devices using the service portal.
- Locked devices are resistant to a very wide range of both physical and software based attacks.
- Bypassing or defeating the software and OS will not enable malicious locking or unlocking of the device at a hardware level.
- Recovering a locked device locally or remotely is only possible by the operator or owner who are provided with a session-specific unlock key from the service portal (following out-of-band authentication).

Connectivity Requirement

- Locking a device following a loss or theft requires Internet connectivity.
- Device auto-locks when it senses a potential physical attack, even if it did not receive a remote lock command.
- Unlocking a device can be done locally (without connectivity).

Constraints or Dependencies

Android OS; requires Internet connection to activate the service.

Impact to Flow

- User is asked to enroll the service during the initial device setup using Setup Agent.
- User can choose not to enroll (opt-out). User can enroll the service later.
- User creates an account and provides some information.
- User can optionally set up an unlock PIN, or one will be randomly generated and stored by the service provider (for later retrieval if device is locked).
- The service is activated.
- The user (and operator) can locate, track, wipe, ring, message, or lock the device from the service portal.

- Advanced users wishing to perform custom OS replacement can deactivate the service and remove the protection.

Level of Accessibility and Funding Model

Available to OEMs on chipsets starting Q2’2015.

Status of Availability

Chipsets available at the beginning of Q2’2015.

Reference URL

https://www.qualcomm.com/products/snapdragon/security.

D.2.8 Samsung

Samsung solution is comprised of two parts “Reactivation Lock” and “Find My Mobile”. “Reactivation Lock” is designed to prevent access to the device after it has been lost or stolen. It uses Samsung account to regain access and use of the device. Samsung account authenticates and authorizes protection of your personal information. “Find My Mobile” allows the user to manage their device by locating, locking, wiping, unlocking and receiving SIM change alerts. Both of these solutions are described in the following subsections.

D.2.8.1 Samsung Reactivation Lock

Non-Technical Description, Capabilities & Functions

- Reactivation Lock prevents device from reactivation on a network after a factory reset.
- When Reactivation Lock is engaged the device will be locked and prevents access beyond the device setup screens.
- Consumer credentials (Samsung account name and password) are required to be entered bypass Reactivation Lock.

Connectivity Requirement

- No connectivity required to engage Reactivation Lock via factory reset from device.
- Connectivity required to engage Reactivation Lock via internet command to force a remote factory reset (Cellular data or WiFi).

Constraints or Dependencies

- Requires consumer Samsung account to be entered on the device to turn on or off solution (requires connectivity).
- Must be activated by the consumer before functionality is available.
- Available only on devices with ARM® TrustZone® architecture.

Impact to Flow

Consumer Response

- Via Samsung Find My Mobile the consumer can factory reset the device to engage Reactivation Lock (any other app which performs a factory reset can also engage Reactivation Lock).

Opportunistic Thief / Criminal Enterprise

- If Thief or Criminal enterprise attempts to factory reset the device, Reactivation Lock would be engaged.

Level of Accessibility and Funding Model

Provided at no cost to consumer on technically capable devices.

Status of Availability

- Some models of Galaxy Note 3.
- Most models of Galaxy S5.
- Additional models to be added for compliance with state laws.

Reference URL

What is Reactivation Lock and how do I use it?

D.2.8.2 Samsung Find My Mobile Solution

Non-Technical Description, Capabilities & Functions

- Web based solution which allows the consumer to remotely access their device.
- Features include the ability to locate, lock, force a factory reset, retrieve call logs, wipe device, get alerts if SIM-card has changed, ring device and enable emergency mode.

Connectivity Requirement

The device must have internet access (Cellular data or WiFi).

Constraints or Dependencies

- A Samsung account must be used.
- Remote control must be enabled on device on prior to use.
- Restricted to Samsung devices.
- Supports Android Gingerbread and above (Android version 2.3).

Impact to Flow

Consumer Response

- User automatically signed up when signing into Samsung Account.
- From website, user can locate, lock (and place notice information on phone and/or set default call back number), force a factory reset, retrieve call logs, wipe device, receive alerts if SIM-card has changed, ring device and enable emergency mode.

Level of Accessibility and Funding Model

No fees to use this service.

Status of Availability

In market since 2011, launched in 130 countries in over 40 languages.

Reference URL

http://findmymobile.samsung.com.

D.3 Third Party Solutions

This section describes a sample of the existing third party solutions available for the prevention of the mobile device theft. The following example third party solutions are described in this section:

- Absolute LoJack
- AT&T Mobile Locate
- Lookout

The descriptions for each of the third party solutions which cover the following topics:

- Non-Technical Description, Capabilities & Functions
- Connectivity Requirement
- Constraints or Dependencies
- Impact to Flow
- Level of Accessibility and Funding Model
- Status of Availability
- Reference URL

D.3.1 Absolute LoJack

Absolute Software Corporation (TSX: ABT) is the industry standard in persistent endpoint security and management for computers, tablets and smartphones. The Company, a leader in device security and management tracking for over 20 years, provides solutions for both consumer and commercial customers.

Absolute's solutions – Computrace®, Absolute Manage®, Absolute Service, and Absolute LoJack® – provide individuals and organizations with actionable intelligence to remotely safeguard, securely manage BYOD, and deliver comprehensive visibility and control over all of their devices and data. Additionally, Absolute provides fully managed Theft Recovery Services working with law enforcement agencies around the globe.

Absolute persistence technology is embedded in the firmware of computers, tablets and smartphones by global leaders, including Acer, ASUS, Dell, Fujitsu, HP, Lenovo, Microsoft, Motion, Panasonic, Samsung, and Toshiba, and the Company has reselling partnerships with these OEMs and others, including Apple. For more information about Absolute Software, visit www.absolute.com.

The solution available from Absolute Software Corporation is called "Absolute LoJack".

Non-Technical Description, Capabilities & Functions

- Absolute LoJack is the only persistent security software system for mobile devices with a Theft Recovery Team that partners with law enforcement globally to recover stolen devices.
- Key features include:
  - **Persistence**: The Absolute Persistent Service (APS) is embedded into the firmware of millions of devices at the factory by the OEM. Once the LoJack software is installed by the end-user on an APS-enabled device, it is extremely resilient to attack, surviving uninstallation attempts including a factory reset of the device.
  - **Remote Location:** Users can remotely locate their device via a web-based portal using GPS, WiFi or IP geolocation.
  - **Device Lock:** Device Lock prevents anyone from accessing the personal user information. Users can also add a custom message to the device lock screen until the user unlocks the device.
  - **Data Delete:** Users can activate the data delete feature to erase sensitive data protecting their personal information and help prevent identity theft.
  - **Device Forensics:** For devices reported as stolen, if the user requests it, the Absolute Investigations & Recovery team can forensically mine a stolen device over the Internet to determine who has the device and what they're doing with it, including determining whether any data was accessed post-theft.
  - **Theft Recovery:** At our customer's request, the Absolute Investigations & Recovery team will work closely with local police to recover a stolen device. The Absolute Theft Recovery team has existing relationships with over 6,500 law enforcement agencies around the globe and successfully recovers thousands of devices each year.
  - **Service Guarantee:** If the stolen device isn't recovered within 60 days, Absolute will help provide compensation for a replacement device. (Some conditions apply.)

Connectivity Requirement

Requires an Internet connection to invoke the remote tracking & security features.

Constraints or Dependencies

- Compatible with major mobile device and PC operating systems including Android OS, Windows OS & Mac OS.
- An Internet connection is required for remote tracking & invocation of security functions.

- Firmware implementation of the Absolute Persistent Service (APS) required by the OEM to provide solution self-healing capabilities enabling Theft recovery & Service Guarantee services.
- Currently pre-embedded on the majority of commercially available platforms being shipped by a number of global OEMs.

Impact to Flow

- Primary audience for purchase of Absolute LoJack are consumer end-users.
- Consumer end-users have access to the web-based Absolute Customer Center Portal where they can install the solution and track and secure their personally-owned device.
- If device goes missing, the end-user can remotely locate the device from the Absolute Customer Center portal, lock the display with a custom message and remotely delete sensitive data on the device via any Internet connection to the device.
- In the event the device is stolen, the end-user files a theft report with local law enforcement and then notifies the Absolute Theft Recovery Team. The Absolute Theft Recovery Team will then conduct remote forensics on the device to determine location, and more importantly, who is using the device working in close contact with the local law enforcement agency.
- With the premium version of the service, 60 days post-loss report to Absolute, in the event the device is deemed non-recoverable or Absolute fails to perform the data delete service, Absolute will compensate the device owner a Service Guarantee of up to $600 for mobile devices. Some conditions apply.

Level of Accessibility and Funding Model

- Absolute LoJack 30-day free trials and annual paid subscriptions are available via www.lojack.absolute.com/en.
- Absolute LoJack is also available for download via Google Play and various other online & offline retail partners.

Status of Availability

- Absolute LoJack and Theft Recovery Services are available globally today.
- Absolute Service Guarantee available in select markets.

Reference URL

- www.absolute.com/en/partners/bios-compatibility.
- www.absolute.com.
- http://lojack.absolute.com/en.

D.3.2 AT&T Mobile Locate

The solution available from AT&T is called “AT&T Mobile Locate” application and is available exclusively to AT&T customers.

Non-Technical Description, Capabilities & Functions

- AT&T Mobile Locate is available for both iOS and Android operating systems.
- AT&T Mobile Locate gives customers the convenience and security of an all-in-one mobile protection solution for your device AND personal data.
- Easily back up contacts, photos and videos no matter where you are. Secure your personal data for free over AT&T's network or Wi-Fi, whether at home OR on vacation.
- With AT&T Mobile Locate, customer's most important data is always protected and accessible through our secure online portal.
- Quickly find a lost phone by locating it on a map from the web, and sound an alarm if it's nearby.
- And, when a customer needs live support, a customer care expert is only seconds away with the click to call feature (available for AT&T Mobile Protection Pack customers).
- iOS Features:
  - CLOUD BACKUP: Sync contacts, photos and videos using Wi-Fi or AT&T network and easily access them from the web.
  - FREE DATA: Your data plan will not be charged if you backup using AT&T's network.
  - DATA RESTORE: Restore contacts, photos and videos to a new device - even if it's not an iPhone.
  - CLICK TO CALL: Directly dial a friendly customer care expert from your phone for Enhanced Support.
  - LOSS AND THEFT PROTECTION: Track your device on a map or with an alarm.
- Android Features:
  - LOCK your device to protect its contents from unauthorized users while it is being retrieved.
  - FACTORY ERASE a lost device to keep your data secure.
  - LOCATE provides a GPS based location to retrieve your device.
  - ALARM sounds an audible alarm if you misplace a device nearby – even if it is set to vibrate or silent mode.
  - LOCK your device to protect its contents from unauthorized users while it is being retrieved.
  - BACKUP and RESTORE your personal contacts, photos and videos.
  - ERASE a lost device to keep your contacts, photos and videos secure.
  - FACTORY ERASE a lost device to keep your data secure.

Connectivity Requirement

- Requires iOS 6.0 or later. Compatible with iPhone, iPad, and iPod touch. This app is optimized for iPhone 5.
- Android customers who are OS version 2.2 or higher.

Constraints or Dependencies

AT&T Mobile Locate is available to AT&T customers.

Status of Availability

Available now.

Reference URL

- https://mobileprotectionpack.att.com/.
- https://play.google.com/store/apps/details?id=com.asurion.android.mobilerecovery.att&hl=en.
- https://itunes.apple.com/us/app/at-t-mobile-locate/id456633308?mt=8.

D.3.3 Lookout

The solution available from Lookout is called "Theft Alerts". Theft Alerts is a real time service that intelligently recognizes common actions thieves take after stealing a phone and provides the end-user with timely and contextual information on the whereabouts of their stolen phone. Theft Alerts was designed to deter the phone theft problem.

Non-Technical Description, Capabilities & Functions

- Lookout did its research and identified common actions thieves take after stealing a mobile device, which prevent the user from calling or tracking it. When an action is triggered, within minutes, Theft Alerts sends the victim an email with a photo* of the thief and a map with the exact location of the stolen phone or tablet.

  Actions that trigger a Theft Alert include:
  - Incorrect passcode entered*
  - Removal of SIM card
  - Airplane Mode has been enabled
  - Device powered off*
  - Lookout was removed as the device administrator*
- Some of these actions are performed regularly by the actual owner of a device, so Lookout also allows users to customize their Theft Alerts experience, turning off the triggers they don't want to be alerted on.

*Android only

Connectivity Requirement

Cellular Network or Internet is required for Lookout to send a Theft Alert.

Constraints or Dependencies

All Theft Alerts triggers are available for Android, but due to platform constraints, only Airplane mode and SIM card alerts are available for iOS. Apple also does not allow Lookout to take a photo with the front-facing camera on iOS, so that functionality is only available on Android.

Impact to Flow

- Primary Audience is end user.
- When use opts-in to the feature, they are proactively alerted of suspicious activity on their device and given recommended actions to take (lock, wipe, etc.) and given useful information for reporting the theft (IMEI, carrier info, etc.)

Level of Accessibility and Funding Model

Theft Alerts is now available in Lookout Mobile Security Premium on Android and iOS for $2.99 per month or $29.99 annually.

Status of Availability

Currently available to download from Google Play and iOS App Store.

Reference URL

- https://play.google.com/store/apps/details?id=com.lookout.
- https://itunes.apple.com/us/app/lookout-backup-security-find/id434893913?mt=8.

D.4 Wireless Operator Implementations

This section describes the mobile device theft prevention implementations the following wireless operators:

- AT&T
- Sprint
- T-Mobile USA
- Verizon

D.4.1 AT&T

AT&T supports the focus by law enforcement, elected officials and others on developing a comprehensive approach that will help reduce mobile device theft and help consumers protect themselves from loss of the device and potential harm from these crimes. This comprehensive approach will provide consumers with tools to protect their devices, secure personal data and reduce the incentive for criminals to commit these crimes. Smartphone theft is a national issue with national, and global, implications.

In April 2012, the FCC and AT&T, with cooperation from other wireless carriers, announced plans to create a stolen phone database to deter theft by making stolen phones useless; once a device is reported missing or stolen, AT&T will simply block all its voice and data communications and prevent it from being reactivated.

In addition, AT&T supports the 2013 CTIA Smartphone Anti-theft Voluntary Agreement[70] under which carriers will allow operating systems and equipment manufacturers to develop and implement anti-theft tools for smartphones.

AT&T led the development of and supports the GSMA-NA "Analysis and Recommendations for Stolen Mobile Device Issue in the United States" for wireless operators to share blacklisted (e.g., stolen) mobile device IMEIs through the GSMA IMEI Database.

AT&T mobile device theft prevention is based on the following principles:

- All devices should be sold with the ability to enable the owner of the device to locate, wipe and lock it in the event of loss or theft.
- Wireless operators and others may offer additional protections to consumers to help them further secure their device.
- Wireless operators have created and will maintain a stolen phone database so the identified mobile phones can be blocked or unblocked on all digital networks in the U.S.
  - Lost or stolen phones will become almost worthless for resale purposes since the phone can not be reactivated by anyone but the rightful owner.
- Accelerated efforts to globally link similar databases across carriers and regions to enhance the effectiveness of this tool and mitigate the incentive to export stolen devices to markets outside of the U.S.
- Continued efforts by the wireless industry to educate consumers about measures they should take to secure their devices and their personal data. This includes constant awareness of one's surroundings when using the devices, the importance of passwords or PIN to access the device and how to remotely track, wipe and lock the device.

AT&T has taken a number of other voluntary steps to assist Law Enforcement in mobile device theft prevention initiatives. AT&T is also concerned about unintended consequences, such as a universally mandated technology to render phones inoperable makes those phones susceptible to being compromised and rendered inoperable, individually by hackers or on a wholesale basis by terrorists/hostile nations; state regulation which mandates a particular technological solution disincents future development of other solutions that consumers demand and that might better serve consumers as a whole. The vibrant growth and development of an incredible array of advanced technology in the lightly regulated wireless industry should serve as a reminder of the benefits of letting the market work.

The AT&T's Mobile Device Theft Prevention is a combination of the following:

- Database,
- Device, and
- Wireless Network solutions.

[70] http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

AT&T recommends if a wireless device is lost or has been stolen, the subscriber must suspend the wireless service to prevent unauthorized usage. The AT&T system will recognize the device as 'Stolen' and block that device from use on the AT&T network within 24 hours. A web page[71] is dedicated to reporting of a lost or stolen phone.

AT&T provides its subscribers the ability to quickly suspend service if the phone or device is ever lost or stolen. Tools are provided online for the subscriber to suspend or re-activate service, or they may call AT&T Customer Service. This protects a subscriber's account from unauthorized use until the subscriber can replace the lost or stolen device. There is no charge to suspend or reactivate wireless service. Suspending wireless service on a lost or stolen device:

- Disables all services except for calls to 911 and 611 for Customer Service.
- Service remains suspended until the subscriber reactivates it.
- If the customer is sure the device was stolen, AT&T recommends blocking it to prevent unauthorized voice, text, and data use on the AT&T network if another SIM card is inserted.
- A subscriber can block a device up to 30 days after its last use.

Before suspending service, AT&T recommends attempting to find the device or protect subscriber privacy by using the features below if available:

- **Find your device:** If the subscriber previously activated device-location services or applications like Find my iPhone, AT&T Mobile Locate, or AT&T FamilyMap, the subscriber should see if they can locate the lost or stolen device. Once service is suspended for the device, these features are disabled.
- **Remote screen lock or data wipe:** If the phone has the ability to remotely lock the screen or wipe subscriber data from the phone, use these features before suspending service. Once service is suspended for the device, these features are disabled.

AT&T has created a URL webpage[72] featuring detailed consumer safety tips on what to do if a smartphone is lost or stolen, including:

- Password protect your wireless device as soon as you receive the device.
- Change your online and voicemail passwords often.
- Secure access to your AT&T account by adding a security passcode today.
- Back Up your Contacts! Learn about this and other tips for your device at the AT&T Device How-To Center.

AT&T Mobile Protection Package

AT&T offers its subscribers comprehensive protection for mobile devices. The AT&T Mobile Protection Pack is the most comprehensive level of protection for a subscriber's mobile life. Subscriber information and the device are protected, plus live ongoing support is just a call or click away. Mobile Protection Pack combines Mobile Insurance, Mobile Locate and Enhanced Support.

[71] http://www.att.com/esupport/article.jsp?sid=KB63935&cv=820#fbid=amWEvBQtB2h.

[72] www.att.com/stolenphone.

Mobile Protection Pack

Replace + Locate + Backup + Support

All new customers are provided this link within mobile device fulfillment materials and existing customers are reminded twice per year via messaging.

https://mobileprotectionpack.att.com/web/index.html#stolenphone.

AT&T Mobile Locate App

AT&T offers the AT&T Mobile Locate app to back up and restore personal contacts, photos and videos in the cloud. It also provides the ability to locate a lost device with GPS or an alarm and remotely lock and wipe it to protect the subscriber's privacy.

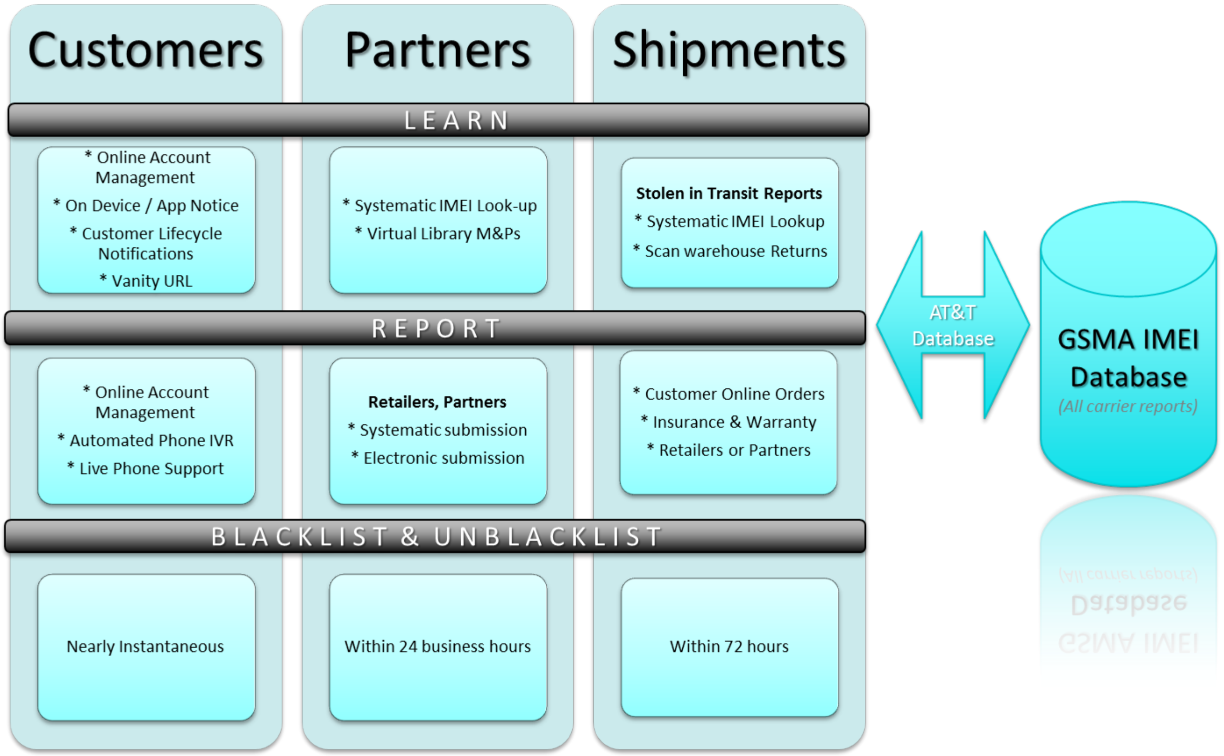
The functionality selected and process for wiping, making inoperable and reactivating the phone should be solely under the guidance and control of the device owner. It should not be controlled by the OS developer, OEM or the wireless provider, and in no case should it be in the control of government officials or law enforcement.

A subscriber's life is on their device. With it containing so much valuable information, subscribers want to make sure to protect the device and data. Quickly locate it if lost, but if stolen, lock the device, back up personal data and erase it to protect privacy. Once the Mobile Locate app is downloaded to the device, a subscriber can tap into their dashboard from any computer to:

- **BACK UP** personal contacts, photos and videos to the secure cloud so they can **RESTORE** as needed.
- **LOCATE** a misplaced device via alarm or GPS.
- **LOCK** it to keep data safe.
- **ERASE** an unrecoverable phone to keep contacts, photos and videos secure.

AT&T End-to-End Solution

AT&T's Mobile Device Theft Prevention solution is an end-to-end solution addressing all stakeholders impacted by mobile device theft.



	Customers	Partners	Shipments
LEARN	* Online Account Management * On Device / App Notice * Customer Lifecycle Notifications * Vanity URL	* Systematic IMEI Look-up * Virtual Library M&Ps	**Stolen in Transit Reports** * Systematic IMEI Lookup * Scan warehouse Returns
REPORT	* Online Account Management * Automated Phone IVR * Live Phone Support	**Retailers, Partners** * Systematic submission * Electronic submission	* Customer Online Orders * Insurance & Warranty * Retailers or Partners
BLACKLIST & UNBLACKLIST	Nearly Instantaneous	Within 24 business hours	Within 72 hours

Figure 16: AT&T End-to-End Solution

- AT&T depends on the consumer to report the device stolen.
  - AT&T encourages the consumer to contact law enforcement in the event of a crime.
- Once the device has been reported, AT&T continually blocks the device from connecting to its network (911 calls are allowed from the device); suspends any AT&T wireless service; and provides a voice recording to the end user to contact the wireless carrier for support if a call is attempted.
  - The architecture depicted is illustrative of solutions on the network to perform this function and may not represent actual deployments.
- AT&T uses the GSMA IMEI Database to check that a device is not listed for every account activation attempt, before any device trade, and during warranty or insurance exchanges.

Alternate EIR (Equipment Identity Register) Solution

AT&T uses the latest in technology to deny service to reported stolen devices reported not only by AT&T customers, but GSM/LTE devices worldwide through the GSMA IMEI Database.

AT&T's deployed technology, both global standards-based and proprietary, helps prevent AT&T smartphones that are reported as lost or stolen from being activated or provided service on our network.

The following diagram is an example of a network-based solution to block service to blacklisted devices.

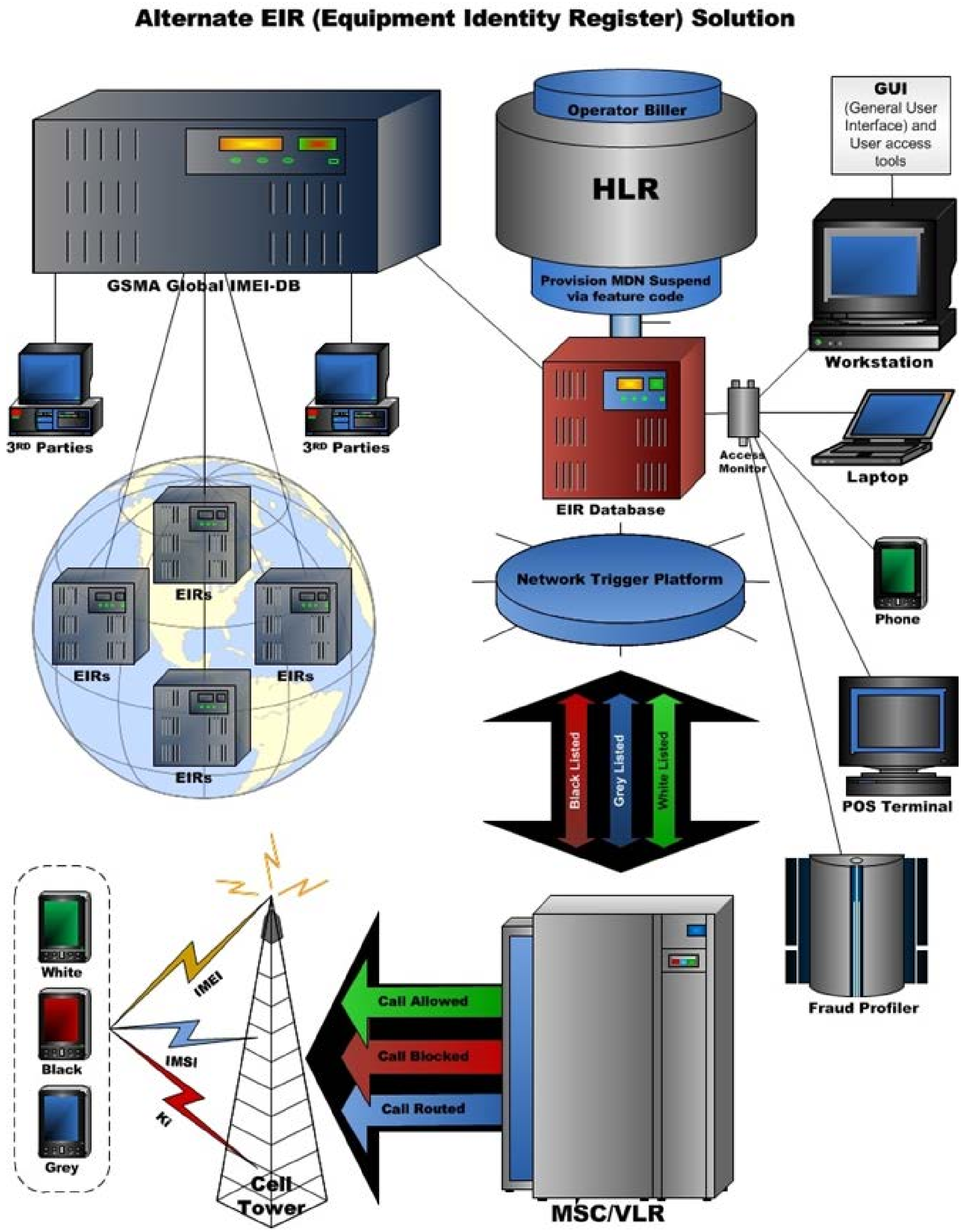


Figure 17: Alternate EIR Solution

D.4.2 Sprint

Sprint shares the concern of the FCC and Law Enforcement that consumers using smartphones or other consumer electronics may be the victim of crime. Sprint has taken a number of steps to implement a voluntary commitment to Law Enforcement to combat smartphone theft, including the implementation of a lost and stolen phones database. Sprint continues to hold detailed talks with OEMs and Operating System vendors such as Google with the objective of delivering a compliant "kill-switch" technology on Sprint devices.

In November 2013, Sprint began sharing lost and stolen data for LTE devices with the international lost/stolen database. The implementation of this international database, which cost the industry millions of dollars, was completed in November of 2013 and the database is now continuing to devalue stolen devices and help reduce the incentive to steal smartphones.

Sprint has also implemented a database that prevents Sprint CDMA smartphones that are reported as lost or stolen from being activated on Sprint's network or provided Sprint services.

Sprint has created a "vanity" URL webpage at www.sprint.com/stolenphone featuring detailed consumer information on what to do if a smartphone is lost or stolen, encouraging the use of passcodes, and highlighting several mobile security apps that can locate, lock and wipe lost or stolen smartphones. For prepaid users, Sprint created similar "vanity" URL webpages for its Virgin and Boost websites.

Sprint has used bill messages, social media, and Sprint's on-device consumer notification application, "Sprint Zone," to encourage the use of passcodes and applications to locate, lock, and wipe smartphones, highlight Sprint's procedures for preventing smartphones that have been reported as lost or stolen from being provided service on our network, and communicate other steps our customers can take to help prevent smartphone theft.

Sprint continues to work cooperatively with the FCC and Law Enforcement on additional ways to protect consumers from smartphone related crime.

Sprint also has taken an active role in helping to prevent smartphone crime by working to fight international, organized, illicit trafficking in mobile devices. This effort includes participation in undercover investigations, lawsuits against identified traffickers, implementing technological changes in the phones to make them harder to traffic, and working with regulators and law enforcement. As part of our aggressive tactics to identify and stop theft and smartphone trafficking, Sprint has sued dozens of traffickers across the country and been awarded tens of millions of dollars in judgments.

Sprint would prefer to see an Operating System solution that works in a uniform manor across all smartphones, as opposed to individual OEM solutions that may have different features and potential vulnerabilities. Sprint is continuing to discuss with industry, including OEM and OS providers, potential "kill switch" technologies that might help to deter Smartphone crime while also addressing potential safety, security, consumer confusion and other vulnerabilities that could also come along with hastily adopted "kill-switch" technology. All current generation Sprint Android and Apple devices provide Sprint customers with free native applications through the device operating systems that provide track/lock/wipe capabilities and audible alarms for lost or stolen devices. Sprint also provides their customers with Lookout Mobile Security on Android devices as a preloaded application.

Sprint has taken a number of steps to protect consumers and combat smartphone theft, including participating in the CTIA Smartphone Anti-theft Voluntary Agreement industry "kill switch" initiative, implementing the GSMA's international lost and stolen phones database, and working with international partners and law enforcement to combat trafficking in stolen devices.

Sprint has an aggressive theft prevention program which includes:

- Joining with the CTIA, major OEMs and the other major carriers in voluntarily agreeing to implement "kill switch" technology on all smartphones manufactured after July 1, 2015.
- Sharing lost and stolen data for LTE devices with the international lost/stolen database.
- Implementing a database that prevents Sprint CDMA smartphones that are reported as lost or stolen from being activated or provided service on our network.
- Submitting its lost and stolen device identification numbers to CheckMEND. CheckMEND is the most complete international listing of lost and stolen mobile devices available and includes data from major wireless carriers and law-enforcement entities globally and allows both consumers and law enforcement to verify the status of Sprint smartphones.
- Creating a "vanity" URL webpage at www.sprint.com/stolenphone featuring detailed information on what to do if a smartphone is lost or stolen, encouraging the use of passcodes, and highlighting several mobile security apps that can locate, lock and wipe lost or stolen smartphones. For prepaid users, Sprint created similar "vanity" URL webpages for its Virgin and Boost websites.
- Using bill messages, social media, and Sprint's on-device consumer notification icon, "Sprint Zone," to encourage the use of passcodes and applications to locate, lock, and wipe smartphones.
- Helping to prevent smartphone crime by working to fight international, organized, illicit trafficking in mobile devices. This effort includes participation in undercover investigations and lawsuits against identified traffickers Sprint has sued dozens of traffickers across the country and been awarded tens of millions of dollars in judgments.

Sprint Mobile device theft prevention implementation.

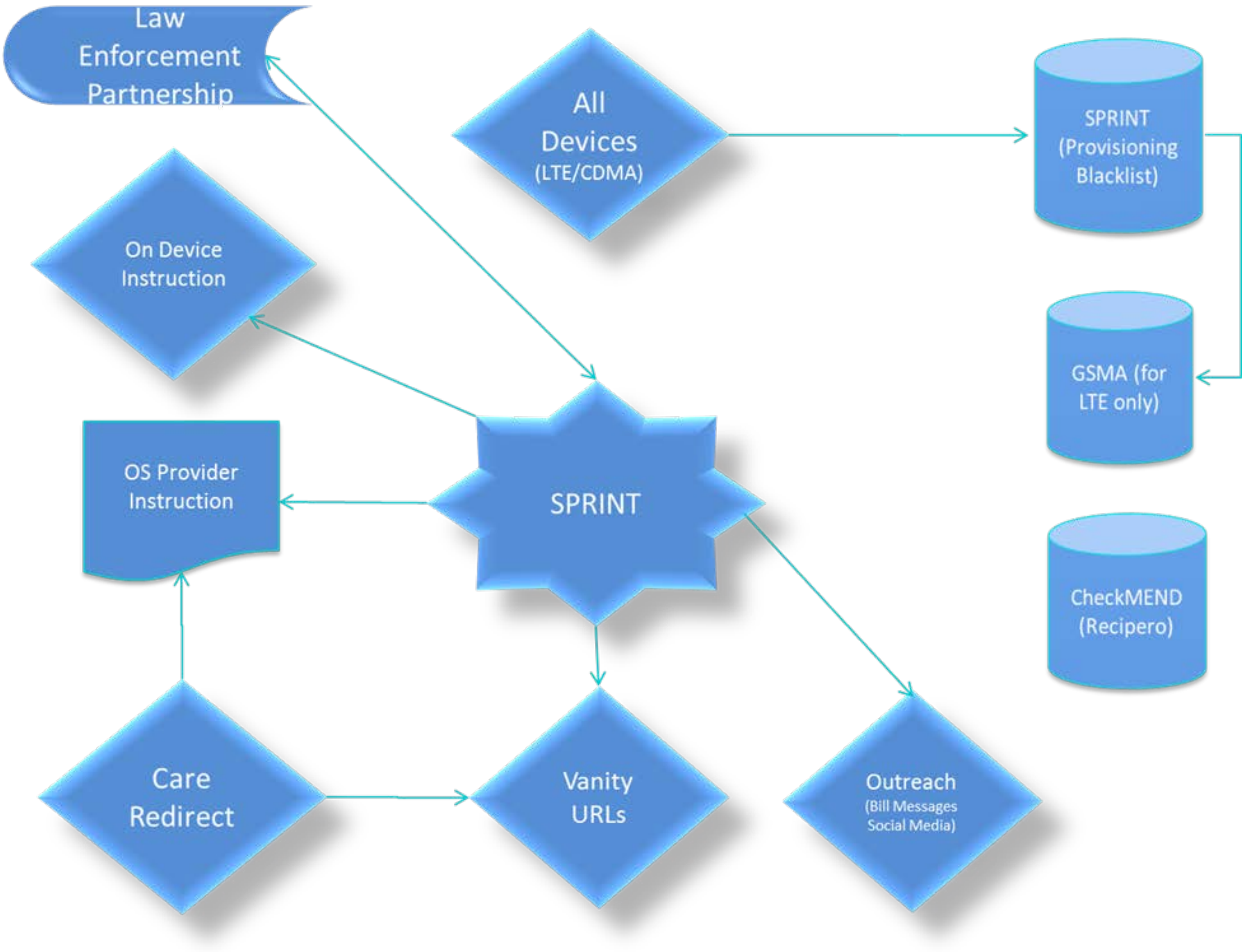


Figure 18: Sprint Mobile Device Theft Prevention Implementation

D.4.3 T-Mobile USA

T-Mobile is concerned about the problem of wireless handset theft. In addition to the anti-theft protections it has already implemented, T-Mobile continues to evaluate and implement additional tools to help end the risks posed to our customers by handset theft, such as technologies that include a "kill switch." T-Mobile believes any such technologies must provide sufficient levels of consumer protection, security, and control to avoid creating other security concerns for consumers. T-Mobile's goal is to develop a comprehensive strategy to empower its customers by enabling an effective and usable solution that deters theft and helps consumers to better protect their devices.

T-Mobile believes the most effective program to mitigate this problem will have a number of components:

- Consumer Education: Consumers are often best situated to prevent theft, by the application of common sense ("situation awareness") and by using the tools currently available, including:

  - Solutions to lock every handset with a Password-protected lock; and
  - The Lookout feature on T-Mobile's handsets to remotely lock and wipe personal data from a stolen handset.
- Strengthen the deterrent effect and expand the reach of the GSMA IMEI Database, in particular by adding foreign carriers to the database.
- Cooperation among the industry, the FCC and local law enforcement officers on reasonable law enforcement initiatives.
- Widespread adoption of technological solutions that are becoming available to deter theft of handsets.

T-Mobile has been at the forefront of the wireless industry's efforts to deter handset theft.

- Handsets sold by T-Mobile include security software (supplied by Lookout) that allows subscribers to remotely locate and lock a lost or stolen handset, as well as to erase the subscriber's confidential data from the handset.
- T-Mobile actively participates in industry-wide programs to deter handset theft. Along with other wireless carriers, handset manufacturers and CTIA, T-Mobile worked with the Federal Communications Commission and the Major City Police Chiefs to develop a program to deter handset theft, culminating in a Voluntary Commitment between the FCC and the members of CTIA dated April 10, 2012.
- In October 2012, T-Mobile established connectivity to the GSMA IMEI Database, where stolen devices are listed on a centralized database in an effort to prevent their use on another carrier's GSM/LTE network. (T-Mobile's work on the IMEI Database is ongoing, as it evaluates options to strengthen the deterrent effect of the IMEI.)
- T-Mobile continues to participate in discussions with Federal, State and Local governments, in order to develop initiatives to combat the problems associated with handset theft.
- T-Mobile is working with Operating System Vendors and handset manufacturers to ensure that additional effective anti-theft functionality ("kill switch") is preloaded on smartphones T-Mobile will sell in the second half of 2015. It is expected that these anti-theft technologies will have the capability to render the essential features of a stolen smartphone inoperable and to withstand a hard reset.

The following diagram depicts the mobile device theft prevention implementation by T-Mobile USA:

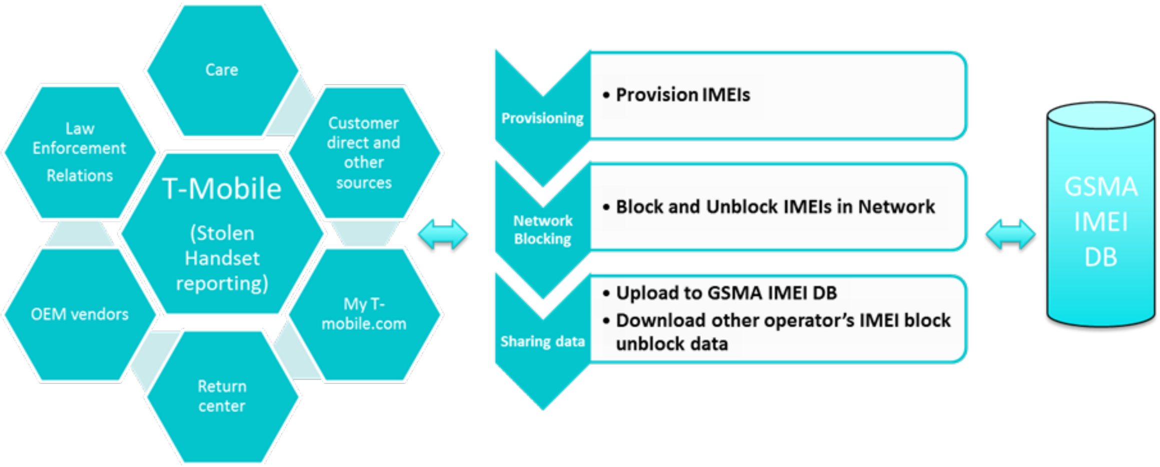

Care
Law Enforcement Relations
Customer direct and other sources
T-Mobile
(Stolen Handset reporting)
OEM vendors
My T-mobile.com
Return center
Provisioning
• Provision IMEIs
Network Blocking
• Block and Unblock IMEIs in Network
Sharing data
• Upload to GSMA IMEI DB
• Download other operator's IMEI block unblock data
GSMA IMEI DB

Figure 19: T-Mobile USA Mobile Device Theft Prevention Implementation

D.4.4 Verizon

Verizon is concerned about the theft of its customer's mobile devices and has worked diligently with CTIA, policymakers and law enforcement to develop the proactive, multifaceted approach of databases, technology, consumer education, legislation and international partnerships to remove the aftermarket for stolen phones.

Verizon Wireless began its customer education campaign in 2012 by launching a consumer-focused web page on Verizonwireless.com that provides customers with information on the prevention of smartphone theft, the importance of using passwords to protect data on smartphones, and what to do if a smartphone is lost or stolen. The site can be accessed at the following link: (http://aboutus.verizonwireless.com/wirelessissues/phonesecurity.html). The site provides direct links to:

- Handset manufacturers' app stores where customers can download anti-theft applications.
- Registration for the company's Wireless Workshops. These classes are offered online and in stores to new and existing Verizon Wireless smartphone customers and are intended to educate customers on the wide array of powerful features and applications, including security measures.

Verizon Wireless also included information on how to safeguard smartphones and the data on them in the company's monthly newsletter, which is emailed to its customers. Also, as part of its "welcome email" communications program, Verizon Wireless advises new customers on the availability of passwords and other safety measures to protect the data on their smartphones.

Additionally, Verizon Wireless has offered since 2012 an application for Android smartphones, also now available for newer Apple devices, called Verizon Mobile Security. Reaffirming Verizon Wireless' commitment to robust security, Verizon Mobile Security helps customers protect their devices from digital threats and equips customers with the power to remotely locate, alarm, lock, and even wipe data from a misplaced or lost device. Developed in partnership with Asurion and McAfee, Verizon Wireless has made this application available in Google Play and iTunes App Store. Details can be found at: http://www.verizonwireless.com/mobilesecurity.

Verizon Wireless' long-standing commitment to deterring crime includes preventing reactivation on its network of all smartphones that its customers have reported to it as lost or stolen. When a customer reports a lost or stolen smartphone, Verizon Wireless adds that smartphone to its "negative list" file. Verizon Wireless' "negative list" was developed for phones that use its CDMA network, and helps Verizon Wireless prevent the reactivation of any CDMA smartphone that is compatible with the Verizon Wireless network and has been reported to the carrier as lost or stolen. Verizon Wireless supplemented its protections by launching a network solution that prevents ongoing use of 4G LTE smartphones that have been reported as lost or stolen to the carrier or the industry-wide GSMA IMEI Database, even if an already-active SIM card is inserted into the device. Verizon Wireless is participating in the industry-wide GSMA IMEI Database to share information it receives on stolen devices.

Verizon also supports the CTIA Smartphone Anti-theft Voluntary Agreement under which carriers will allow operating systems and equipment manufacturers to develop and implement anti-theft tools for smartphones.

The following diagram depicts the end-to-end mobile device theft prevention implementation by Verizon:

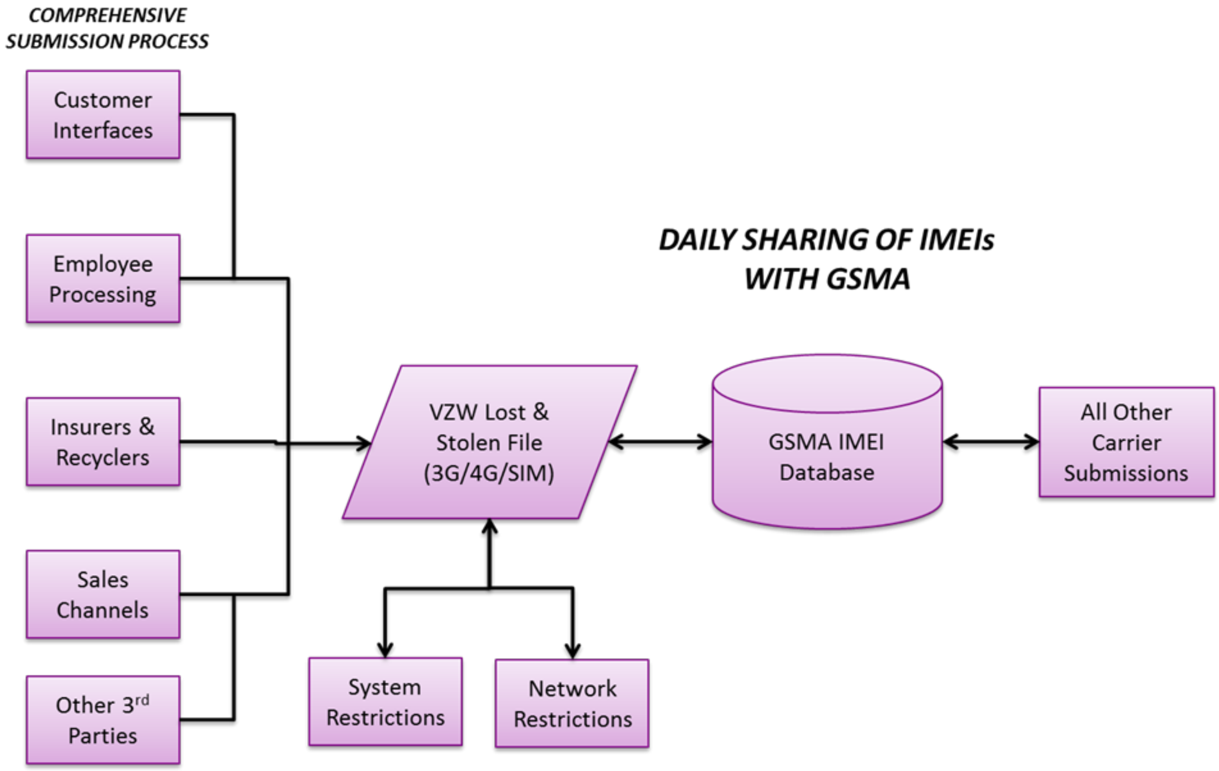


Figure 20: Verizon End-to-End Mobile Device Theft Prevention Implementation

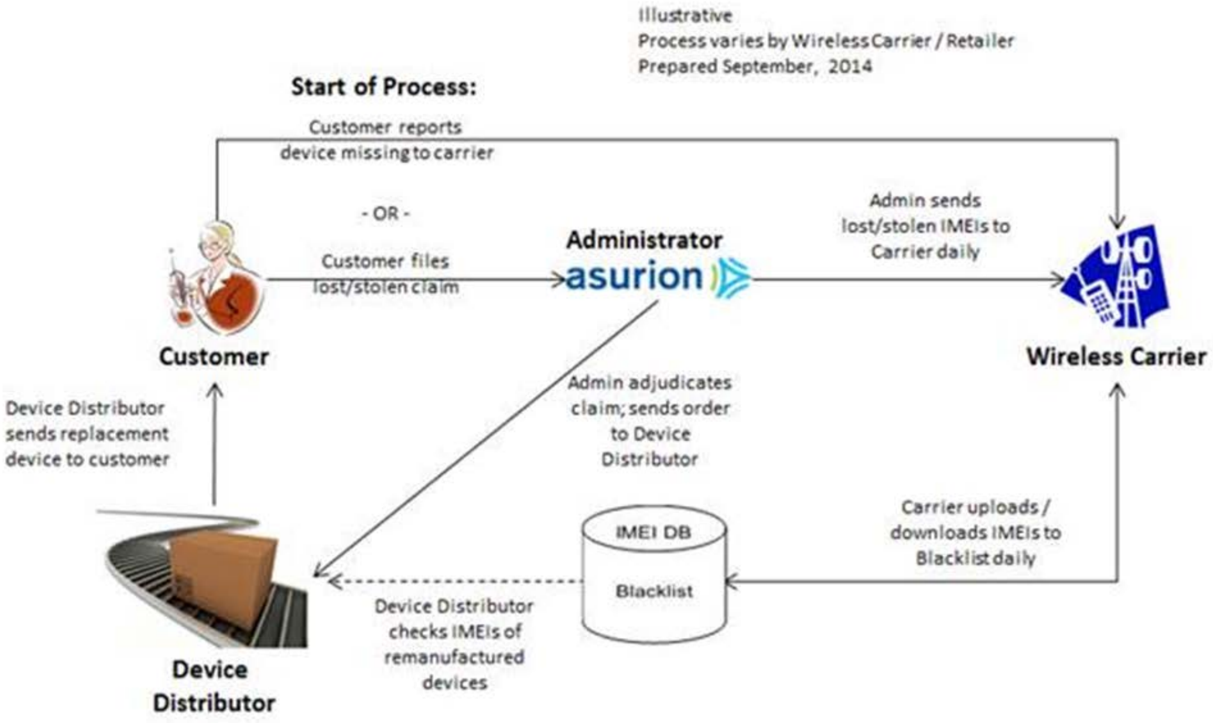
D.4.5 Carrier Insurance Programs

Asurion is an administrator for device insurance programs offered by wireless carriers. Examples of carrier device insurance programs include the list below. Additional details may be viewed at the URLs shown. These programs are all in market as of the publication of this document.

- AT&T Mobile Protection Pack (MPP) at https://mobileprotectionpack.att.com.
- Sprint Total Equipment Protection (TEP) at https://protection.sprint.com.
- Verizon Total Mobile Protection (TMP) at https://totalmobileprotection.verizonwireless.com/.

MPP, TEP and TMP provide protection for the customer in the event the device is lost, stolen, damaged, or malfunctions. Customers contact Asurion for help with their device, including filing a claim if the phone is lost or stolen, and may be determined eligible to receive a replacement device the next day.

The figure below is an illustrative information flow for lost/stolen claims made to Insurance Administrators such as Asurion.


Illustrative
Process varies by Wireless Carrier / Retailer
Prepared September, 2014
Start of Process:
Customer reports device missing to carrier
- OR -
Customer files lost/stolen claim
Administrator
asurion
Admin sends lost/stolen IMEIs to Carrier daily
Customer
Wireless Carrier
Admin adjudicates claim; sends order to Device Distributor
Device Distributor sends replacement device to customer
IMEI DB
Blacklist
Carrier uploads / downloads IMEIs to Blacklist daily
Device Distributor checks IMEIs of remanufactured devices
Device Distributor

The process generally works as follows:

Asurion reports claim events to wireless carriers through systems integrations, including noting when phones are reported as stolen.

Wireless carriers aggregate info from Asurion's claims CRM with carrier's own stolen devices records, and then the carrier reports to GSMA.

Asurion and other Device Distributors leverage the GSMA IMEI database to verify that devices in queue to be used as replacement phones have not previously been reported as stolen.

Note that Asurion informs the carrier that the device was reported as lost or stolen. Asurion also recommends to the customer that he/she inform their carrier directly to expeditiously stop data/voice services. The Carrier then corroborates Asurion's info and relays a single source of truth to GSMA.

There are a couple of key limitations to the information available in the insurance programs. First, many wireless customers whose phones are lost or stolen are not customers of an insurance program. Additionally, many customers who subscribe to protection programs inform the wireless carrier of a lost/stolen event prior to informing Asurion.

Customers who have enrolled in TMP, MPP or TEP are charged a monthly fee on the carrier's monthly bill, and customers remit payments as a part of their payment for voice, data, etc. TMP, MPP and TEP are typically available for all devices within first 30 days of purchase, and at periodic open enrollment windows.