Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) Analysis and Recommendations for 2015

Version 1.0

4 December 2015

Table of Contents

Executive Summary

Industry has invested significant resources and effort to develop mechanisms to help smartphone owners reduce the impact of smartphone theft and to assist their recovery if they fall victim. The United States has led the world in seeking device based solutions and initiatives such as the FCC TAC MDTP Working Group efforts, cellular providers voluntary commitment to deploy database solutions, the CTIA's Smartphone Anti-Theft Voluntary Commitment, and the introduction of legislative provisions in California and Minnesota have been particularly instrumental in facilitating and promoting the emergence of a range of anti-theft features. The availability of anti-theft features on all smartphones is expected to increase following the effective date of the CTIA Voluntary Commitment, and the California and Minnesota laws.

Analyzing trends in consumer usage and obtaining an empirical understanding of consumer usage patterns will provide a data-driven basis for determining whether any further action is needed to increase customer usage of anti-theft features and, if so, provide a clear understanding of factors that either encourage or discourage consumer use. In doing so, remedial efforts can be targeted to resolve empirically identified obstacles. The effectiveness of device blocking on mobile networks is dependent on the secure implementation of device identities. Enhanced device identity integrity is essential to the efficient and effective network blocking of stolen mobile devices. Significant efforts were made to improve device identifier security with real commitment and engagement by the device manufacturing community. These led to a series of initiatives that have been central to improved device identity security levels.

Mobile technology standards provide that mobile identities must be unique per device and that they must be protected against alteration after the point of manufacture. No details or guidance are provided as to how exactly these security goals are to be achieved. Following detailed analysis, industry concluded that standardization is unsuitable as a means to deal with device identity issues and that incorporating enhanced security features in the standards could be problematic and undesirable. Standardizing the technical means to protect device identities could expose devices to even greater risk if the prescribed safeguards are compromised as that would expose all devices if one method fits all.

Currently, OEMs and chipset suppliers have different security implementations, some better than others, but mandating a single solution would most likely remove the enhanced level of protection offered by some manufacturers.

The GSM Association (GSMA) led the development of two major industry initiatives designed to enhance the security of mobile device identity implementations. Twenty-one of the largest device manufacturers formally signed up to support both initiatives in 2005. The number of devices with vulnerable identities had decreased by 77%, the number of manufacturers with vulnerable products reduced by 45% from 11 to 6, and the number of available and effective hacking tools had shown a 72% decrease. Problems did persist with two manufacturers that, between them, accounted for 83% of compromised device models and their failure to respond appropriately to reported security problems was regrettable.

Modification of device identities is a criminal offence in some jurisdictions but not in the United States where websites and outlets exist, and are on the increase that openly advertise the ability to change device identities. Developers of attacks against device identities are known to be based in the USA, Israel, India, and Eastern Europe.

Across the US, law enforcement officers may not be aware of the significance or existence of the device identifier (IMEI, MEID, etc.). 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. Across the US, law enforcement officers are not fully aware of how to access information that is in the GSMA IMEI Database.

A fragmented system of consumer outreach exists in which no single government agency, group, manufacturer, or carrier providing a uniform and comprehensive outreach program or source for information. Consumers don't always report the theft of their devices to law enforcement and/or carriers. Consumers need instructions and clarity of the process and procedures for the reporting of stolen devices. Potential buyers of smartphones do not have access to complete information 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.

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 comprehensive information.

Timeliness of information is too long and is dependent on reporting frequency as well as upload/download frequencies of most of the databases. Effort is underway within the GSMA to harmonize the practices and policies of blacklisting devices.

Many mobile network operators in other countries do not block stolen services or share relevant data with other operators. Consequently stolen smartphones in those countries could still be operational.

Some US mobile network operators, especially the smaller mobile network operators, do not block stolen devices or share the identities of those devices with other operators or other interested stakeholders.

To address these conclusions, the MDTP Working Group developed thirteen actionable recommendations for consideration and are highlighted in this report.

1 Overview

1.1 Introduction

This overview section provides the report introduction, the mission statement, the scope of work, 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.

1.2 Mission Statement

The FCC TAC Mobile Device Theft Prevention (MDTP) Working Group continued their work from 2014. The emphasis for 2015 is on longer term initiatives that will combat more sophisticated theft scenarios:

- Developing recommendations on next generation anti-theft features.
- Processes including recommendations for hardening of existing device identifiers and the possible need for new, more secure identifiers.
- Security mechanisms with higher consumer acceptance (e.g., biometrics).

- More focused analysis of overall theft ecosystem including how stolen devices re-enter the marketplace (e.g., recycling industry).
- Further recommendations on improved reporting mechanisms.

Consideration will also be given to the efficacy of extending theft prevention mechanisms to other classes of devices.

The MDTP Working Group will provide an assessment of progress made in the area of device theft prevention as some of these recommendations have been applied.

1.3 Scope of Work

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 sufficiently 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

For 2015, the FCC TAC Mobile Device Theft Prevention (MDTP) Working Group initially started development of the following three separate reports:

- Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) on On-Device Theft Prevention Features
- Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) on Hardened Device Identifiers
- Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) Database and Portal Analysis and Recommendations

However, the MDTP Working Group later decided that one consolidated report would be the best deliverable to the FCC. This report is the consolidated working group report.

In 2014, the MDTP Working Group established several sub-working groups. However, for the 2015 work activities, the MDTP Working Group decided not to create any sub-working groups. Instead, the MDTP Working Group agreed to develop all three reports simultaneously during the usually weekly working group conference calls.

1.5 MDTP Working Group Membership

Table 1: MDTP Working Group Membership

Name	Organization
Brian K. Daly, Co-Chair	AT&T
Robert Kubik, Co-Chair	Samsung
Asaf Askenazi	Qualcomm

Name	Organization
Jay Barbour	Blackberry
Bradley Blanken	Competitive Carriers Association (CCA)
Craig Boswell	Hobi
Jeff Brannigan	Department of Homeland Security (DHS)
Mathew Bromeland	Metropolitan Police, Washington, DC
Mike Carson	ebay
Chris Drake	iconectiv
Eric Feldman	ICE/Homeland Security Investigations
Thomas Fitzgerald	New York City Police Department
Les Gray	Recipero
Shelley Gu	Microsoft
Joseph Hansen	Motorola Mobility
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
Deepti Rohatgi	Lookout
Mark Romer	Asurion
Matt Rowe	Gazelle
Christian Schorle	FBI
Ron Schneirson	Sprint

Name	Organization
David Strumwasser	Verizon Wireless
Maxwell Szabo	City and County of San Francisco
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 MDTP database and portal Use Cases, carrier database solutions, and Device Information Portal.
- Section 3 defines the on-device theft prevention features including efforts already in progress, existing commitments and laws, topics for future discussion, and how to increase consumer use of these functions.
- Section 4 provides the considerations for the hardening of the device identifiers.
- Section 5 contains the recommendations.
- Appendix A is the Glossary.
- Appendix B provides additional information regarding information aggregator database solutions.

2 MDTP Database and Portal

2.1 Use Cases

This section provides the use cases and is organized into the following subsections:

- Law Enforcement Use Cases
- Consumer Use Cases
- Resellers of 2nd Hand Devices Use Cases

2.1.1 Law Enforcement Use Cases

Story Highlights

Law enforcement has the need to identify the status of a mobile device which has been reported stolen by the owner, or has been recovered or otherwise in possession by law enforcement. Status of a device for the purposes of law enforcement includes whether the device has been reported lost or stolen to the service provider last providing service to

that device; whether the device is on a "blacklist" identifying it was reported lost or stolen; the enrollment status of on-device theft prevention solutions; whether an individual with whom law enforcement comes into contact is the rightful owner of the smartphone.

Use Case: Victim reports stolen device to law enforcement

Primary Actor(s): Law Enforcement Officials.

Preconditions: Law enforcement has been made aware that a mobile device was stolen through the victim reporting it stolen. Victim has already reported the stolen device to the service provider, service to the device has been suspended, and the service provider has put the device identifier on a blacklist. Victim is cooperating with law enforcement. Device is enrolled in an anti-theft solution.

Basic Flow:

1. Law enforcement asks the victim for information about the cell phone:
    a. Make, model.
    b. Phone number assigned to the cell phone.
    c. Device identifier (IMEI, MEID).
    d. Service provider.
    e. Type of anti-theft solution and enrollment status of the anti-theft solution.
2. Law enforcement uses appropriate information sources to verify:
    a. Blacklist status of the device identifier (IMEI, MEID).
    b. Enrollment status of the on-device anti-theft solution.
    c. Verify the device make/model.
    d. Identify the service provider.
    e. Other history as available.
3. Law enforcement asks the user to use their anti-theft solution's "locate" feature, if available, to see if a location of the device can be obtained.
    a. If the device can be located, follow internal procedures for further investigation and recovery.
4. If the on-device anti-theft solution cannot provide location, law enforcement may contact the device owner's service provider, or other service providers, to further aid in the investigation according to internal policy and procedures. This may include:
    a. Verify the IMEI as provided by the victim.
    b. Determine if the device has been used on any network since the theft.

Use Case: Law Enforcement comes into possession of a cell phone

Primary Actor(s): Law Enforcement Officials.

Preconditions: Law enforcement comes into possession of a cell phone. Status of the cell phone may be unknown – it may be lost, stolen, or otherwise discarded. Owner of the cell phone is unknown.

Basic Flow:

1. Law enforcement performs a visual inspection of the recovered cell phone to attempt to determine:
    a. Make, model.
    b. Service provider – for example, through device labeling or on-screen information.
    c. Device identifier (IMEI, MEID) – potentially using a series of keystrokes to display the identifier, or if the device is "locked" through an anti-theft solution, attempt procedures to obtain the device identifier.
    d. Enrollment status of the anti-theft solution.
    e. Device owner if the owner has a lock screen message providing identifying information.
2. Assuming the device identifier was obtained, law enforcement uses appropriate information sources to obtain additional information about the device:
    a. Blacklist status of the device identifier (IMEI, MEID).
    b. Enrollment status of the on-device anti-theft solution.
    c. Verify the device make/model.
    d. Verify the service provider.
    e. Other history as available.
3. Law enforcement may use this information to contact the service provider to further aid in the investigation according to internal policy and procedures.

Use Case: Law Enforcement comes into possession of one or more cell phones in the field

Primary Actor(s): Law Enforcement Officials

Preconditions: Law enforcement comes into possession of one or more cell phones in the field. Status of the cell phones may be unknown – they may be lost, stolen, or otherwise discarded. Owners of the cell phones are unknown.

Basic Flow:

1. Law enforcement performs a visual inspection of the recovered cell phones to attempt to determine:
    a. Make, model.

b. Service provider – for example, through device labeling or on-screen information.

c. Device identifier (IMEI, MEID) – potentially using a series of keystrokes to display the identifier, or if the device is "locked" through an anti-theft solution, attempt procedures to obtain the device identifier.

d. Enrollment status of the anti-theft solution.

e. Device owner if the owner has a lock screen message providing identifying information.

2. Assuming the device identifiers were obtained, law enforcement uses field tools to access the appropriate information sources to obtain additional information about the devices:

f. Blacklist status of the device identifier (IMEI, MEID).

g. Enrollment status of the on-device anti-theft solution.

h. Verify the device make/model.

i. Verify the service provider.

j. Other history as available.

3. Law enforcement may use this information to contact the service providers to further aid in the investigation according to internal policy and procedures.

Use Case: Law Enforcement comes in contact with smartphone robbery victim

Primary Actor(s): Law Enforcement Officials, Victim.

Preconditions: Law enforcement responds to mobile device theft incident. Law enforcement has been made aware that a mobile device was stolen. Victim is cooperating with law enforcement. Device is enrolled in an anti-theft solution.

Basic Flow:

1. At the crime scene, law enforcement asks the victim for information about the cell phone:

a. Make, model.

b. Phone number assigned to the cell phone.

c. Device identifier (IMEI, MEID).

d. Service provider.

e. Type of anti-theft solution and enrollment status of the anti-theft solution.

2. Law enforcement uses field tools to access the appropriate information sources to verify:

f. Blacklist status of the device identifier (IMEI, MEID).

g. Verify the device make/model.

h. Identify the service provider.

i. Other history as available.

3. The victim will contact the service provider to provide notification of the theft. Law enforcement should remind the consumer to do so. The service provider suspends his subscription and the device identifier is placed on the lost or stolen phone blacklist.
4. When the victim is able to access the Internet, the victim uses the features of their anti-theft solution such as remote lock, wipe, and locate.

Additional Law Enforcement Considerations

The following are additional considerations that impact the law enforcement use cases:

1. Across the US, law enforcement officers may not be aware of the significance or existence of the device identifier (IMEI, MEID, etc.)
2. Procedures to obtain the IMEI or MEID 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 policies 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 a service 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.

Example of a Law Enforcement Investigative Guide for Finding a Stolen Cell Phone

The Seattle Police Department has developed an Investigative Guide for How to Find a Stolen Cell Phone[1]. The redacted version of this investigative guide is presented for illustrative purposes in the following figure which spans two pages.

[1] http://www.seattle.gov/Documents/Departments/Police/manual/06_140_locating_cell_phone(0).pdf

SEATTLE POLICE INVESTIGATION GUIDE

FIND A STOLEN CELL PHONE

(EVEN AFTER IT IS WIPED AND ISSUED A NEW NUMBER!)

by Detective Christopher Young
Seattle Police Criminal Intelligence Section
[redacted]

IS THIS A LIFE OR DEATH EMERGENCY?

YES!

Follow procedures under SPD manual section 6.140 – Locating a Cell Phone during an Emergency [redacted]

NO!

The victim may have reported the phone stolen to his or her provider, however history has shown that people have been able to get "blacklisted" phones working, so you should proceed even if it is reported stolen.

IS THE MISSING PHONE A SMARTPHONE THAT CAN BE TRACKED ONLINE?

YES!

Have the victim go online and log into his or her account at the appropriate web site:

Android (Galaxy, Droid, etc.)
google.com/android/devicemanager
iOS (Apple iPhone)
icloud.com
Windows Phone (Nokia)
windowsphone.com

Keep in mind that if you want the phone company to give you information directly, generally you need a court order.

NO!

Do you know the victim's cell service provider (i.e AT&T/Verizon/T-Mobile)?

YES!

CAN YOU LOCATE THE PHONE VIA GPS?

YES!

Go look for the phone and associated thief! Keep in mind that you will need to evaluate your need for a warrant as the search progresses--for example, if you believe that the device is in a residence.

NO!

Use the Number Portability Check by calling [redacted]

NO!

Have your victim sign a Consent to Search form (form 9.54) as the carriers may require written permission from the account holder.
Call the victim's service provider and ask:
1) Has the victim's phone been used since was stolen?
&
2) What's the phone IMEI (International Mobile Station Equipment Identity) ?
Find carrier contact info here:
http://www.search.org/programs/hightech/isp/
The phone's number may have been changed since it was stolen, but the IMEI will remain the same. For technical reasons, it is easier to keep a phone on the same network, so always check with the victim's phone company first.

IS THE PHONE BEING USED ON THE VICTIM'S NETWORK WITH THE VICTIM'S PHONE NUMBER?

YES!

NO!

You will then need to check other networks, one at a time, by process of elimination.

Determine the network capability of the victim's phone--CDMA, GSM, or World. This can be accomplished by asking the victim's service provider or doing an internet search of the model number of the phone.

93% of cell phones run on a Big 4 Network (Verizon, AT&T, Sprint and T-Mobile) so it is only feasible to check these companies. Verizon and Sprint use CDMA phones.

AT&T and T-Mobile use GSM phones.

World phones work on any network. Notable examples are the iPhone 4S and later. Also the flagship phones (i.e. most expensive) from the Android manufacturers generally are world phones.

THE BIG 4 CONTACT INFO

Verizon Wireless Legal Compliance
[redacted]

AT&T Wireless
[redacted]

Sprint/Nextel Communications, Inc.
[redacted]

T-Mobile
[redacted]

BASIC CONCEPTS

1. The motive for the theft of a cell phone usually is economic, therefore it is likely that it will be sold.

2. If someone pays money for a phone they are going to use it.

3. If a phone is being used on a cellular network, it can be tracked.

4. Sophisticated criminals are able to outwit these techniques by changing the phone's IMEI or shipping it overseas, but most criminals are not sophisticated.

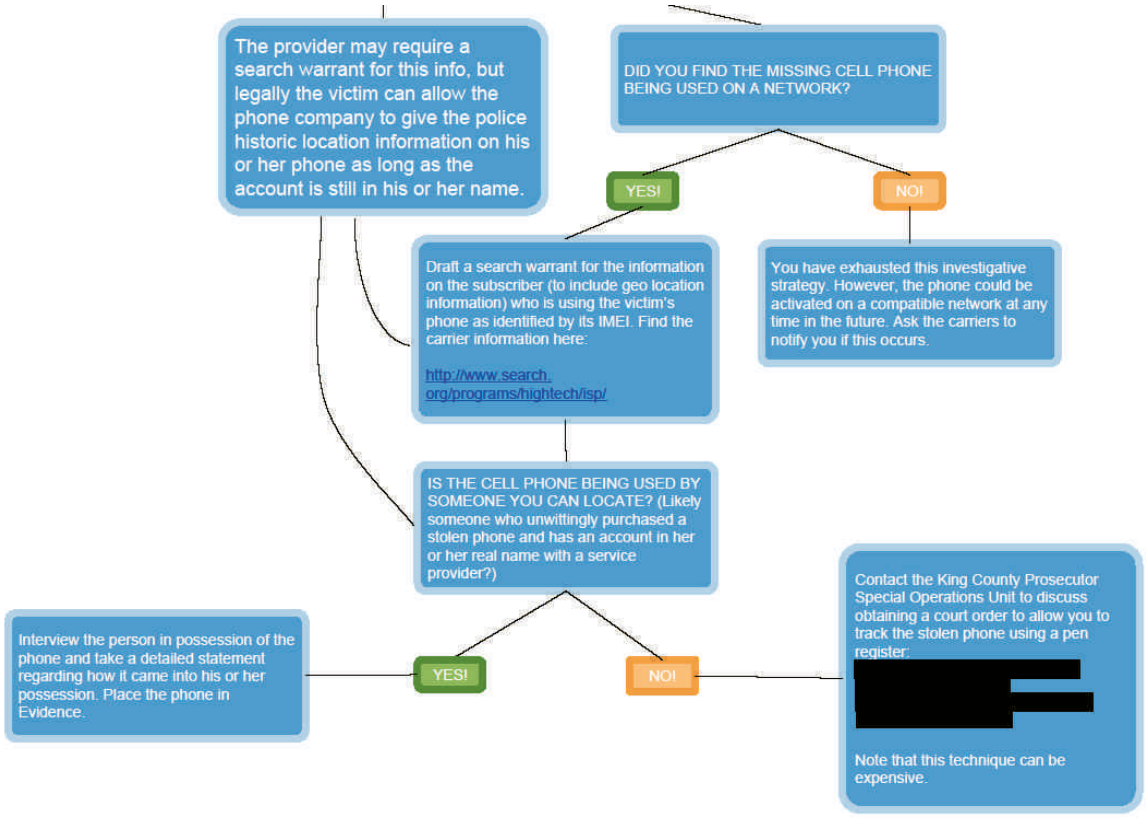

Figure 1: Seattle Police Department Investigative Guide for How to Find a Stolen Cell Phone (redacted)

2.1.2 Consumer Use Cases

Story Highlights

When a device is lost or stolen, consumers have the need to activate on-device anti-theft solutions, and report the lost or stolen device to the service provider and law enforcement (if a crime was committed).

Consumers also have the need to identify the status of a mobile device which is either owned by the consumer, or a device which the consumer is considering purchasing from a reseller or private party. Status of a device for the needs of consumers includes whether the device is on a "blacklist" identifying it was reported lost or stolen; and the enrollment status of on-device theft prevention solutions.

Use Case: Consumer's device is lost

Primary Actor(s): Bob (consumer).

Preconditions: Bob has lost his cell phone and cannot find it.

Basic Flow:

1. Bob has lost his cell phone and since he cannot locate it, he is concerned about someone else finding it and using his subscription to run up his cell phone charges. Bob wants to be sure this is prevented.
2. Bob goes to his service provider's web site and locates information on what to do if his device is lost.
3. Bob follows his service provider's recommended process, which includes:
    a. Bob activating the on-device anti-theft solution to lock the device.
    b. Bob using the "locate" function to attempt to find the device's location.
4. The "locate" function did not return the device location. Bob notifies the service provider the device cannot be found. The service provider suspends his subscription and the device identifier is placed on the lost or stolen phone blacklist.
5. Bob wants to make sure his device is really shut down, and uses appropriate information sources to verify the status:
    a. Blacklist status of the device identifier (IMEI, MEID).
    b. Enrollment status of the on-device anti-theft solution.
    c. Verify the device make/model.

Use Case: Consumer's device is stolen

Primary Actor(s): Bob (consumer).

Preconditions: Bob's cell phone is stolen.

Basic Flow:

1. Bob has his cell phone stolen, either from his person or stolen from the location where he left it. Bob is concerned about the theft, and the perpetrator using his subscription to run up his cell phone charges. Bob wants to be sure this is prevented.
2. Since Bob was the victim of a crime, Bob immediately calls the police to report the crime. Bob may further work with police to attempt to use the "locate" capability of the on-device theft prevention solution to see if the device location is available. The police take the crime report, and urge Bob to contact his service provider.
3. Bob goes to his service provider's web site and locates information on what to do if his device is stolen.
4. Bob follows his service provider's recommended process, which includes:
    a. Bob activating the on-device anti-theft solution to lock the device.
    b. Bob using the "locate" function to attempt to find the device's location.
5. The "locate" function did not return the device location. Bob notifies the service provider the device cannot be found. The service provider suspends his subscription and the device identifier is placed on the stolen phone blacklist.

6. Bob wants to make sure his device is really unusable by an unauthorized user as a cellular phone and uses appropriate information sources to verify the blacklist status of the device identifier (IMEI, MEID).

Use Case: Consumer wants to purchase a cell phone through online reseller

Primary Actor(s): Bob (purchaser), Alice (seller).

Preconditions: Bob has found a cell phone for sale through a local reseller, Alice. The cell phone is the make and model he wants, but he needs to know if this is a legitimate cell phone.

Basic Flow:

1. Bob, being an intelligent consumer, asks Alice information about the device he is interested in purchasing:
    a. Make, model.
    b. Device identifier (IMEI, MEID).
    c. Type of anti-theft solution and enrollment status of the anti-theft solution.
2. Bob obtains the device identifier and uses appropriate information sources to verify information provided by Alice:
    a. Blacklist status of the device identifier (IMEI, MEID).
    b. Enrollment status of the on-device anti-theft solution, if available.
    c. Verify the device make/model.
3. Bob uses the information obtained from the information sourced to make an intelligent purchasing decision.

Use Case: Consumer wants to purchase a cell phone through a storefront or private party

Primary Actor(s): Bob (purchaser), Alice (seller).

Preconditions: Bob has found a cell phone for sale through a local reseller, Alice. The cell phone is the make and model he wants, but he needs to know if this is a legitimate cell phone.

Basic Flow:

1. Bob is interested in purchasing a device that Alice has for sale. Alice agrees to allow Bob to inspect the device before purchase.
2. Bob inspects the device in order to obtain:
    a. Make, model.
    b. Device identifier (IMEI, MEID).
    c. Type of anti-theft solution and enrollment status of the anti-theft solution.
3. Through this inspection, Bob obtains the device identifier and uses appropriate information sources to verify the device status:

a. Blacklist status of the device identifier (IMEI, MEID).
b. Enrollment status of the on-device anti-theft solution.
c. Verify the device make/model.

4. Bob uses the information obtained from the information sources to make an intelligent purchasing decision.

Additional Consumer Considerations

Consumers may have a variety of contractual or commercial relationships on a single device including but not limited to: their device's manufacturer; the provider of the operating system on the device (and upstream providers); their carrier; and providers of anti-theft solutions. As a result, consumers may require education at the time of sale on whom to contact when their device is lost or stolen.

Consumers may feel comfortable in enrolling their smartphone in a program meant to help them find it when lost but may not feel comfortable enrolling their smartphone in a program that will treat all loss events as "theft".

Simply enrolling in an anti-theft solution like Reset Protection or Find My iPhone and Activation Lock is not in any way indicative that their device is or isn't stolen. It is a consumer's decision to opt-out of their anti-theft feature and that decision should remain private.

The following are additional considerations that impact the consumer use cases:

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 or source for information.
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.

   Note: 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. Doing so would raise multiple privacy issues that would need to be accounted for and are outside of the scope of this document but would need to be resolved before enabling an anti-theft solution that updates a centralized database or notifies a mobile service provider and the consumer.

2.1.3 Resellers of 2nd Hand Devices Use Cases

Story Highlights

Resellers have the need to identify the status of a mobile device which is presented to the reseller for recycling, either individual devices or bulk devices. Status of a device for the needs of resellers includes the service provider providing the device subscription, the

make/model of the device, whether the device is on a "blacklist" identifying it was reported lost or stolen; and the enrollment status of on-device theft prevention solutions.

Use Case: Device presented to a reseller for recycling

Primary Actor(s): Bob (consumer), Reseller (person or kiosk).

Preconditions: Bob has a cell phone he wishes to sell to a recycler.

Basic Flow:

1. Bob has obtained a new cell phone from his carrier and wants to recycle his old device with a reseller.
2. Bob goes to the reseller's kiosk, website or storefront with the device he wishes to recycle.
3. The reseller asks Bob for information about the device, and if possible performs a visual inspection of the device to attempt to determine:
    a. Make, model.
    b. Service provider – for example, through device labeling or on-screen information.
    c. Device identifier (IMEI, MEID) – potentially using a series of keystrokes to display the identifier, or if the device is "locked" through an anti-theft solution, attempt procedures to obtain the device identifier.
    d. Enrollment status of the anti-theft solution.
4. Using the device identifier, the reseller uses appropriate information sources to obtain information about, and the status of, the device, including:
    a. Service provider.
    b. Device make/model.
    c. Blacklist status of the device identifier (IMEI, MEID).
    d. Enrollment status of the on-device anti-theft solution, if available.
5. Based on this information, the reseller can make a decision on whether it will recycle the device for Bob.

Use Case: Bulk devices are presented to a reseller for recycling

Primary Actor(s): Reseller (person or kiosk).

Preconditions: Recycler has received a shipment of a large number of devices for recycling/reselling.

Basic Flow:

1. A reseller/recycler has received a bulk shipment of a large number of devices for recycling or reselling.

2. The reseller inventories each device and tries to obtain as much information as it can on each device, including:
    a. Make, model.
    b. Service provider – for example, through device labeling or on-screen information.
    c. Device identifier (IMEI, MEID) – potentially using a series of keystrokes to display the identifier, or if the device is "locked" through an anti-theft solution, attempt procedures to obtain the device identifier.
    d. Enrollment status of the anti-theft solution.
3. Using the device identifier, the reseller uses appropriate information sources to obtain information about and the status of each device, including:
    a. Service provider.
    b. Device make/model.
    c. Blacklist status of the device identifier (IMEI, MEID).
    d. Enrollment status of the on-device anti-theft solution.
4. Based on this information, the reseller can make a decision on whether it will recycle the devices.

Additional Reseller Considerations

1. May be required to adhere to diverse local laws regarding reporting of property taken in.
2. In some cases, no laws or best practice exists and resellers are on their own to conduct business as they see fit.
3. Not all ecommerce sites check databases to check the status of the devices being taken into the ecommerce site.

2.1.4 Portal for Information Aggregation

1. There is no single location for users to obtain instructions on how to report their phone as stolen or on how to retrieve information regarding the status of their phone.
2. 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.
3. 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/MEID Database may be obtained within minutes or once every 24 hours, depending on how frequently carriers upload and download their device data.

4. Authorized users may not understand the importance of identifiers and how to identify their smartphones.
5. 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.

Not all theft prevention solutions may provide an electronic means for a potential buyer to determine whether or not a smartphone is enrolled in a theft prevention solution prior to buying a device.

It is important to note that 'data' is a broad term; not all data is relevant to a stolen phone scenario. For example, OS manufacturers may store device or OS-specific metadata (e.g., color, OS version, OS-specific identifiers, etc.) that has no bearing on any stolen phone or IMEI/MEID blacklists.

2.1.5 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 or those that may be stolen elsewhere and shipped into the US although the latter is not considered likely to be a significant issue.

2.1.6 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. Many mobile network operators in other countries do not block stolen devices or share data pertaining to them. Consequently stolen smartphones in those countries could still be operational.
3. Some US mobile network operators, especially the smaller mobile network operators, do not block stolen devices or share the identities of those devices with other operators or other interested stakeholders.
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 at one location prior to purchase or trade.

Different solutions have different ends by design. Databases and associated network technologies deployed by carriers are to deny service to stolen phones on their networks; databases maintained by OS developers or third party software developers may be to help find lost devices or disable their reactivation. It is not feasible to try to combine these databases – with their different schemas, designs, and end goals – and may result in a net reduction in enrollment across databases if consumers are uncomfortable with having their device enrolled in one solution resulting in their smartphone and identity being accessible by multiple parties far removed from any one of their existing relationships.

Alternative solutions exist, whereby, instead of having a singular database, it is possible for each database to expose to consumers and third parties whether a device is enrolled in a theft prevention system.

If there are consequences outside the customer's control of the customer using anti-theft features, they'll be less apt to use for fear of unintended consequences. Industry and the MDTP Working Group wants to encourage the use of anti-theft tools but taking control of information away from any user of the feature will make users less likely to use these tools. Meanwhile, making enrollment overly onerous will also reduce the use of theft deterrent solutions, thereby exacerbating the theft epidemic.

It is also important to note that device status information stored in separate databases maintained by OS and OEM manufacturers, is by design to protect a user's privacy. Although manufacturers and OS providers aren't directly subject to CPNI rules, those rules identify a type of information that Congress and the FCC have determined are private and should be protected as such. That type of information includes information relating to the technical configuration of the telecommunications service, information relating to the way that a consumer uses their service, etc. When it comes to anti-theft features, OS providers and manufacturers maintain a trusted position with the customer. Given the private nature of the information, the MDTP Working Group strongly opposes any recommendation for OS providers or manufacturers to disclose that private information.

Activation of theft prevention features should be as easy as possible without compromising the trusted position between the consumer, the OS providers, and the manufacturers.

2.2 Carrier Database Solutions

Database solutions may be characterized into the following categories:

- Databases used by network operators containing device identifiers which are used to deny access to known stolen devices on their networks.
- IMEI/MEID Database provided by the GSMA to facilitate the sharing and distribution of stolen device identities between mobile network operators.
- OEM/OS vendor databases which specify the enrollment state of the on device theft prevention solution.
- Aggregator databases which provide device checking services and/or portals to network operator and OEM/OS vendor databases.

The network operator databases are specifically targeting and denying use of known stolen devices on the network. These network operator databases provide the identities of devices stolen from their customers to the GSMA's IMEI/MEID Database for distribution to other network operators and they are independent of the subscriber-initiated enrollment status of their chosen on-device theft prevention solution.

The status of the device within the network operator database and the GSMA Database as well as OEM/OS vendor solution enrollment is important to law enforcement, resellers, insurers, traders, and other third parties involved in the device lifecycle.

2.2.1 Scope of Database Effort

1. The MDTP Working Group is asked to study database systems that effectively track stolen items and develop a specification sheet for an effective stolen phone database that might be focused on North America.
2. GSMA already hosts a configurable stolen phone database which is facilitating pan operator blocking and information distribution. There is an opportunity for ecosystem participants to make greater use of this resource through optimized configuration and adoption.

2.2.2 GSMA IMEI/MEID Solution

The GSMA's IMEI/MEID Database is based on a data platform operated and maintained by the GSMA and is accessible to users through arrangements made directly with the GSMA. The GSMA Database is designed to share stolen device data between network operators to enable them to prevent known stolen devices from being used on any operator network that subscribes to the GSMA Database and that has the necessary technology in place within its network to check for and deny service to blacklisted devices. From the stolen device data contained within the GSMA Database, GSMA also provides a flexible suite of services related to device identity and anti-theft systems, and these are made available to a range of participants in the mobile ecosystem and law enforcement agencies. The GSMA Database also serves as a source of statistical data on device theft and it can make information available to a range of suitable organizations, including regulatory and national authorities.

The GSMA Database contains mobile device status information provided by some mobile network operators. Its blacklist is a list of IMEIs that are associated with mobile devices that should be denied service on cellular networks because they have been reported as lost or stolen. The GSMA Database acts as a central system for cellular operators to share their individual blacklists so that mobile devices denied service (blacklisted) by one network will not work on other networks even if the SIM card in the device is changed. When consumers report to their operator that a mobile device is lost or stolen, operators block the device on their mobile network, rendering it inoperable, and send the information to the GSMA's IMEI blacklist registry. GSMA makes blacklist data to other operators so that devices may be blocked nationally and internationally by operators who use the data in an Equipment Identity Register (EIR) or other systems within their networks.

Operators agree to collect the necessary information relating to their subscribers' lost and stolen devices, and blacklist such devices in accordance with agreed policies and procedures, and to upload to the GSMA Database the identities of those that have been lost or stolen. Similarly, a

network operator may retrieve (download) a list of blacklisted mobile devices from the GSMA Database and operators who implement methods, such as an Equipment Identity Registers (EIR), to deny service to blacklisted mobile devices on their network can use the GSMA IMEI/MEID Database to augment their own lists of blacklisted mobile devices.

The GSMA Database takes the blacklists from the various operators around the world that are connected to the system and it compiles the data into one global blacklist. When a network operator EIR subsequently connects to the GSMA Database, it downloads the latest global blacklist (or a national or regional subset of the global list) for its own use. By loading the blacklist onto the local EIR, all handsets reported as stolen on other connected networks up to the last data exchange are now also capable of being blocked on that network.

Operators who connect to the GSMA Database from time to time may request a full copy of the Blacklist data uploaded to the database by the operators from which they choose to take data. Such an upload can be used to synchronize their local databases with the live system and the relevant data will be provided by the GSMA by email or direct download.

The participating US network operators agree to undertake to blacklist devices within an agreed and defined period from having been notified of IMEIs that have been placed on the GSMA Database blacklist to minimize the risk of resale and reuse of lost and stolen devices.

Currently, information from operators is shared with the IMEI/MEID Database every 24 hours. However, law enforcement would like the information to be uploaded on a more frequent basis and GSMA is working with operators to encourage the upload of blacklist entries to the GSMA Database on an hourly basis with blacklist entries also to be downloaded hourly. This change is a relatively minor software enhancement in some operators' networks but may be more difficult in others. Although industry is committed to the quickest possible exchange of stolen device data, moving to a "Real Time" device blocking and GSMA Database uploading and downloading is more problematic as checking and verification procedures have to be followed and the entire process involves many more systems within the operator's network. Exploring this enhancement is for further study.

The following figure from the GSMA North American Regional Interest Group (GSMA-NA) "Analysis and Recommendations for Stolen Mobile Device Issue in the United States"[2] depicts the sharing of blacklisted IMEIs by two network operators using the GSMA Database:

[2] GSM Association North America Regional Interest Group (GSMA-NA), NAEIR_01, *Analysis and Recommendations for Stolen Mobile Device Issue in the United States*, 1 May 2012.

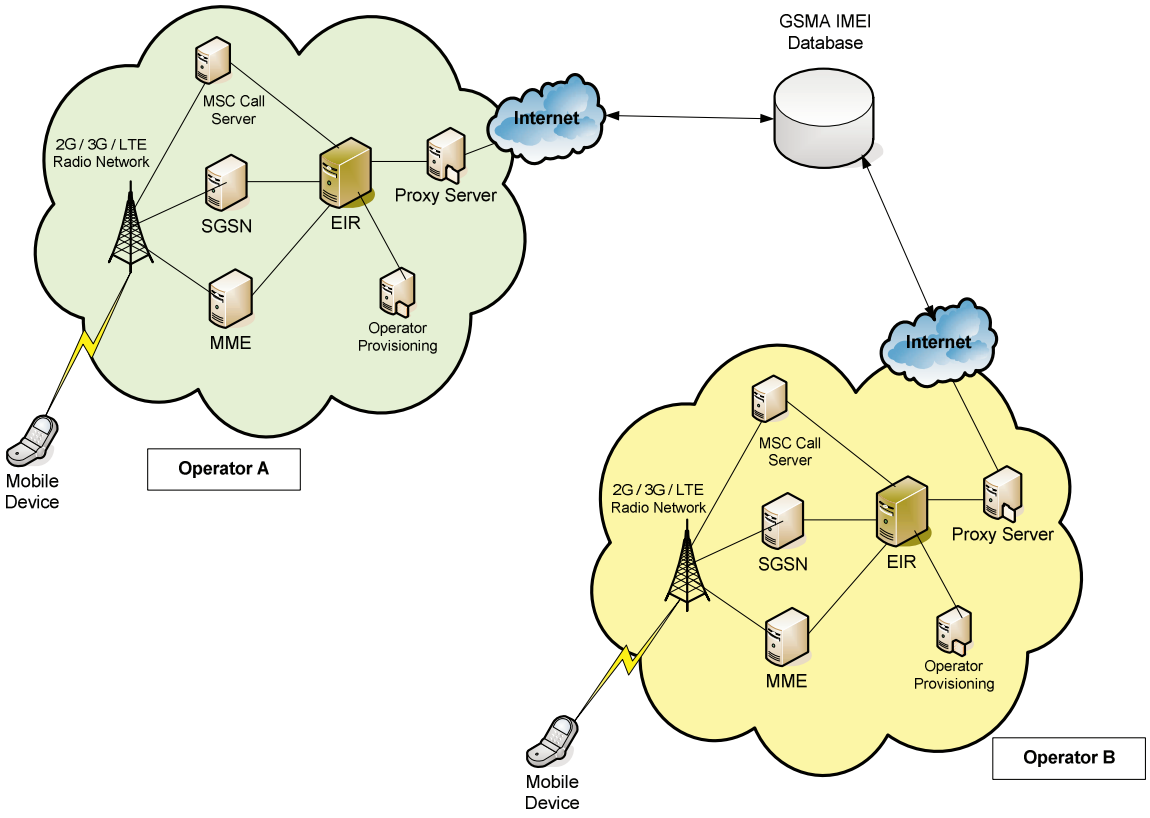

Figure 2: Cellular Operator EIR with GSMA IMEI/MEID Database Connectivity

2.2.2.1 Operator Use of GSMA IMEI/MEID Database

The following example implementations that can be used by the network operators to deny services for stolen mobile devices are described in the GSMA's North American Regional Interest Group "Analysis and Recommendations for Stolen Mobile Device Issue in the United States"[2] and are summarized in this section:

- CDR Analysis Based
- Network Transaction Trigger
- Equipment Identity Register

The procedures for adding a mobile device to a blacklist and for handling of blacklisted mobile devices within a cellular operator's network are operator specific, and work is currently underway within the GSM Association to harmonize the practices and policies, where possible. Cellular operators have many tools and options available to deny service to blacklisted mobile devices.

The following process flow diagram from the GSMA's North American Regional Interest Group "Analysis and Recommendations for Stolen Mobile Device Issue in the United States"[2] shows a typical process for the blacklisting of IMEIs where the subscriber directly reports the stolen mobile device to the cellular operator, and how the data is provided to and shared among cellular operators using the GSMA IMEI/MEID Database:

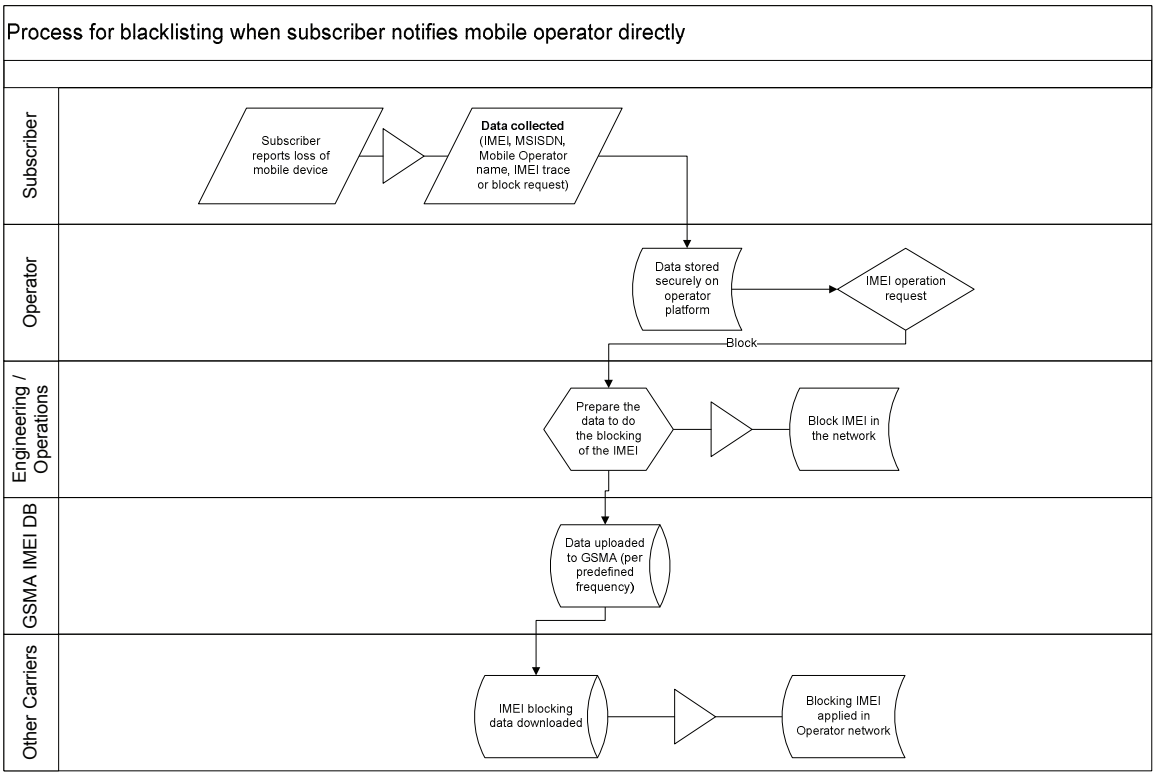

Figure 3: IMEI Blacklisting Process Flow

2.2.2.1.1 CDR Analysis

Call Detail Record (CDR) analysis is an example of a technique that could be used to identify stolen mobile devices to which service should be denied as an alternative to using an EIR.

Whenever a mobile device performs a transaction such as placing a voice call, the cellular operator's network generates CDR records for that transaction. These CDR records, which include the identity of devices in use, are periodically transferred to the cellular operator's billing systems. The billing system could compare the received device identity contained in CDR records against the list of stolen mobile devices and can generate a report of activity by stolen mobile devices. Based upon these reports, the cellular operator can either manually or automatically update their cellular network to deny future service by the identified stolen mobile devices.

2.2.2.1.2 Network Transaction Trigger

Whenever a mobile device is requesting or performing services, a series of transactions occur on the cellular operator's network. The 3GPP standards have defined trigger points in these transactions where a cellular operator may choose to have an application server examine and perhaps modify a transaction in progress. The EIR based example described in section 2.2.2.1.3 is one example implementation of this network triggering capability.

However, a cellular operator may elect to use other trigger points for interaction with servers. When the server receives transactions from other trigger points, the server could compare the IMEI of the mobile device associated with this transaction with the list of stolen IMEIs. If an

IMEI is found to be on the list of stolen mobile devices, the server can respond with an indication that the transaction should be denied and could update the cellular operator network to deny future service to the stolen mobile device.

2.2.2.1.3 Equipment Identity Register (EIR)

The implementation of an Equipment Identity Register (EIR) by a cellular operator is the most common network-based implementation to identify and prevent the use stolen mobile devices. The EIR is a standards-based network infrastructure implementation that has been defined by the 3rd Generation Partnership Project (3GPP), the global standards development organization for the GSM family of technologies.

When a mobile device is powered on, its IMEI is transmitted to the cellular network. During the network registration process, the IMEI is checked against the network's EIR. If the result of the EIR check indicates that the mobile device has been blacklisted (e.g., stolen), registration on the cellular operator network will be denied.

The following figure provides a high level depiction of the location of the EIR within the network architecture:

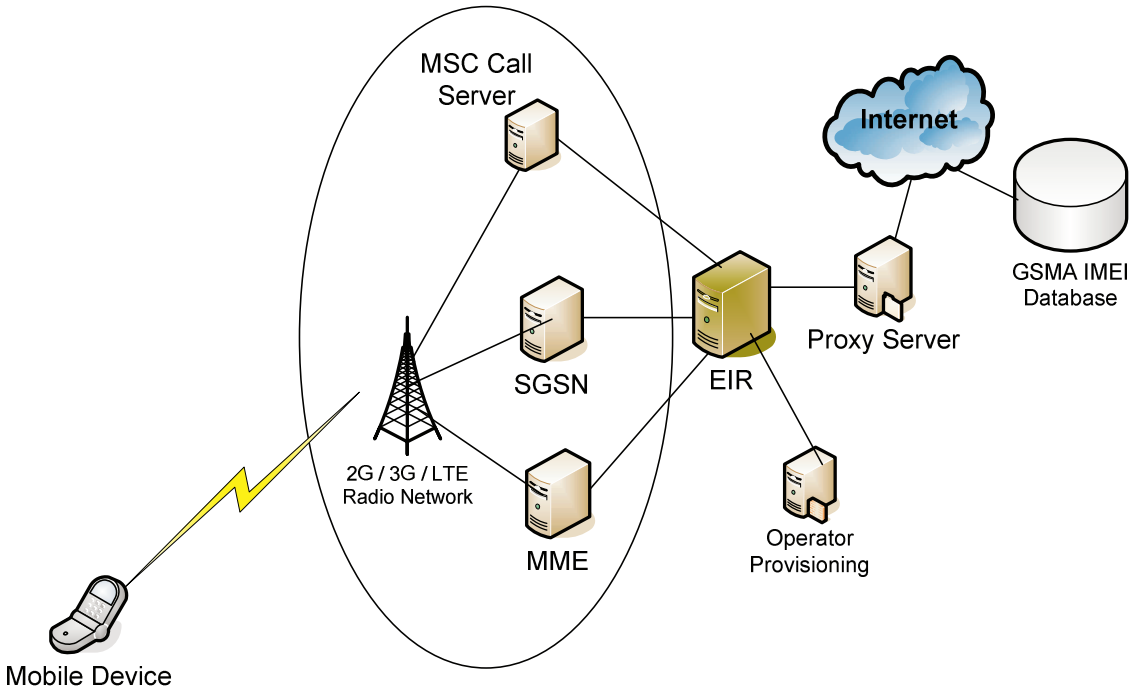

Figure 4: EIR Location within Network Architecture

2.2.3 Identified Gaps in GSMA Solution

- Many carriers around the world and in the USA do not block devices and do not participate in stolen device sharing initiatives.

- Consumers do not always report stolen devices to their service providers to have them blocked.

For device blocking and data sharing to be truly effective thefts need to be reported to carriers that then need to block those devices and share them with other carriers via GSMA's IMEI/MEID Database.

2.3 Non-Carrier Database Solutions

The 2014 FCC TAC MDTP working group report[3] at Appendix D.1 provides information about the non-carrier database solutions. Appendix B of this 2015 MDTP report provides additional information about the information aggregator database solutions.

2.4 Proposed Device Information Portal

For purposes of definitions for this section:

- Information Portal: a specially designed web resource that brings information together from diverse sources in a uniform way for ease of access and availability.
    - "Lost or stolen" – In the context of this document refers to a device that has been reported to a cellular service provider as no longer in the device owner's possession, i.e., through loss or theft. The IMEI/MEID is uploaded to the GSMA IMEI/MEID Database by the cellular service provider. It does not include devices enrolled in OEM/OS programs or the use of those OEM/OS programs. In addition, this does not refer to a device that a user is not in possession of and has not been reported to a service provider.
    - "Data" – In the context of this document, referring to the minimum set of information that is pertinent to lost or stolen devices. This includes IMEI/MEID as standards-based and industry-adopted identifiers. In addition, information about whether the device is enrolled in an OEM/OS program or information about how to access enrollment status. (See Table 1 below).
    - "Other Data" – Information that goes beyond the minimum set of Data pertinent to the device.
    - "Enrollment Status" – Information regarding whether a device is enrolled in an anti-theft tool. (See October 2015 update to the CTIA Smartphone Anti-Theft Voluntary Commitment.)

2.4.1 Problem Definition

The information regarding a device is dispersed across different existing solutions such as the GSMA IMEI/MEID Database, Operator Databases & Blacklists, OEM/OS Databases,

---

[3] [3] *Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP)*; Version 1.0; 1 December 2014; http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf.

Retailer/Reseller Databases, Insurance Databases, Law Enforcement Databases, Customs Databases, etc. Some of these databases are publicly accessible today but a consumer needs to lookup more than one database to obtain all the pertinent information regarding a device such as lost/stolen status, lock status, resold status, etc.

The FCC TAC defines the near term problems as the following:

- Consumers lack a consolidated view of and guidelines from where to obtain device information. This could be to validate that the device that was lost/stolen is indeed on the blacklist or that the device they plan to buy is not blacklisted or locked.
- Consumer education is lacking – Users need instructions and clarity of the process and procedures for the reporting of lost/stolen devices. A fragmented system of consumer outreach exists in which no single government agency, group, manufacturer, or carrier providing a uniform and comprehensive outreach program.
- Lack of information and guidelines for commercial entities such as Resellers, Recyclers, and Insurance companies. For example, Resellers need to access device status information to confirm a device conforms to the recycler's practices before buying the device from a customer. It is not warranted that a reseller validates IMEIs with Operator/GSMA blacklists so junk devices are not resold. Similarly, Recyclers and Insurance companies need a credible source to validate device information.
- Lack of information and guidelines for Law Enforcement Agencies - Not all LEA jurisdictions across the country have the training on how to use the tools to lookup the status of a device to verify if it is a blacklisted or check the enrollment status of the status device.

To summarize, there is a need to have tools and documented best practices in place that provide consumers, LEAs and commercial stakeholders with a clear picture regarding the device information in the United States. This idea is similar to what has been done in Canada[4].

A Device Information Portal enables consumers to get information on how to determine the status of a device using a convenient source. Commercial stakeholders can now validate device information from a credible secure source. Not only does this protect them against liabilities, it also prevents fraud and has the potential to significantly reduce the trade in, and value of, stolen devices making them less attractive to thieves. This solution would also enable law enforcement to obtain timely stolen device information that could be used to nab thieves, potentially retrieve devices and also provide convenient verification of stolen device status at a crime scene.

These checks and balances would reduce the opportunity to trade stolen devices which could help reduce mobile device theft levels and potentially prevent stolen devices from being traded in and out of the country. The portal could also be used as a vehicle for consumer outreach and alerts regarding device security, and be a common national portal for all device status information.

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

2.4.2 User Categories

The Device Information Portal could be utilized as a platform to provide consumers with instructions on how to obtain information about their device and do so by transparently aggregating available device information across different solutions (GSMA, Operator, OEM platform, OS platform and other aggregators) to enable credible, synthesized information to all stakeholders in the mobile ecosystem.

There are three primary categories of users with specific device information requirements as shown in Table 2 below:

- Public
- Commercial
- Law Enforcement

The role of the user will dictate access restrictions (such as limited queries per day/hour, reCAPTCHA codes, programmable access, etc.) and the disclosure of device information.

Table 2: Device Information List for Key User Categories

Device Information Checklist					
	Device Make and Model Details	**Blacklist Status**	**Enrollment Status (or Web Link)**	**Service Provider**	**Timestamp (when the device was blacklisted)**
Public		X	X		
Commercial	X	X	X	X	X
Law Enforcement	X	X	X	X	X

The portal will provide the following views based on the user category and inputted identification number such as the IMEI (for GSM/LTE devices) or ESN/MEID (for CDMA devices):

1. Consumer view: Directions to support pages from various carriers, manufacturers, and/or operating system providers from where users can obtain instructions on how to determine the state of their device, and, to the extent the following information is programmatically available from authoritative sources, information regarding device activation and blacklist (e.g., reported lost/stolen to officials) status.
2. LEA view: In addition to the above information, Operator/Service Provider and a timestamp when the device was blacklisted will be provided. This will enable them to contact the appropriate Service Provider, if required, and also estimate the time when the device was stolen. The make and model of device to which the IMEI applies can also be provided.

3. Commercial view: In addition to the information provided to Consumers, Operator/Service Provider and a timestamp when the device was blacklisted will be provided. The stolen device information will enable commercial entities to avoid fraud and volunteer information to the law enforcement regarding a stolen device. The make and model of device to which the IMEI applies can also be provided.

Additional consumer outreach information including mobile device security warnings and directions could also be provided. The Portal could also be used to provide basic trends & analytics data to the FCC regarding mobile device theft and the impact of the policies to prevent device theft.

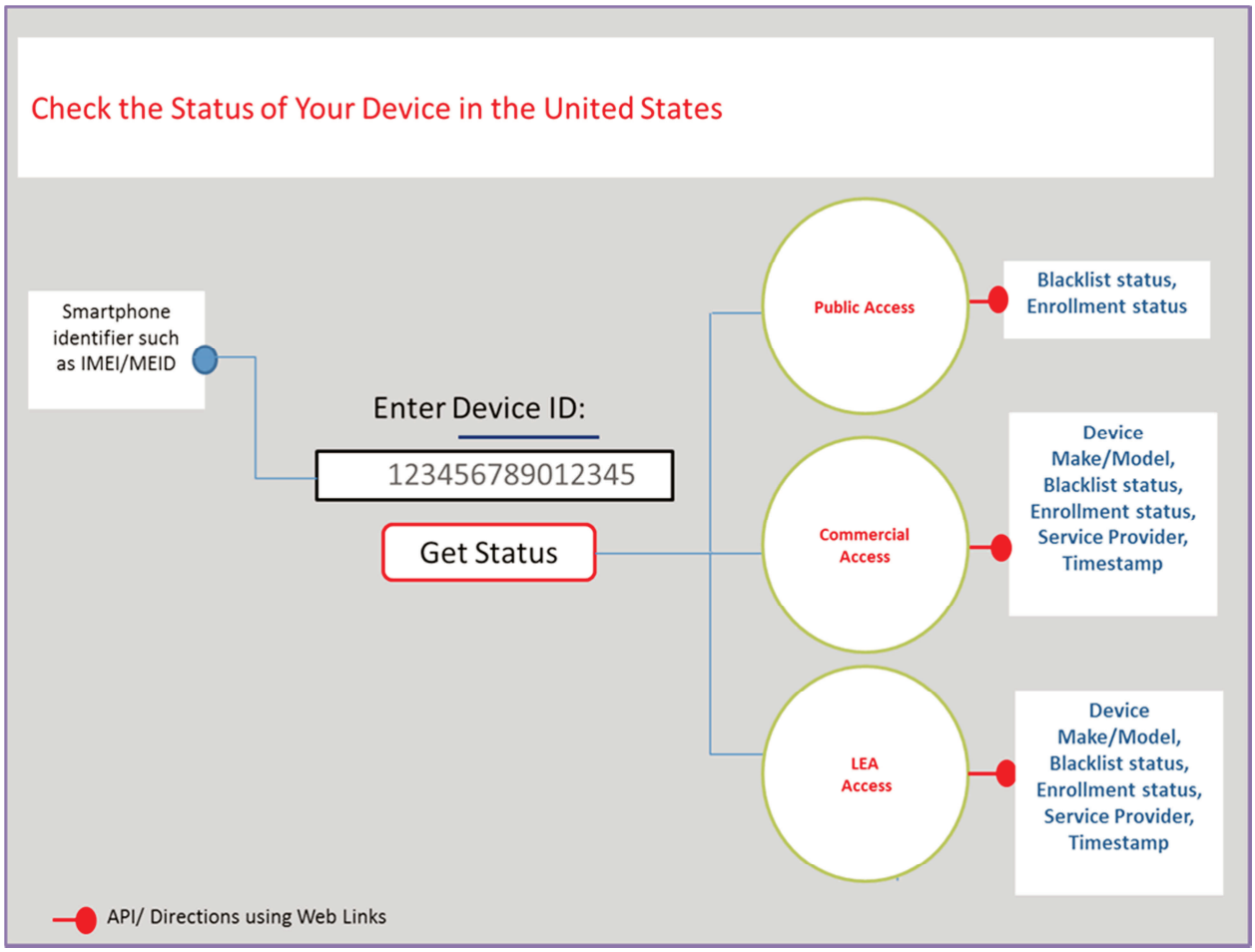

Figure 5: Device Information Portal (Conceptual View)

2.4.3 Issues for Future Discussion

This section summarizes the long term problems that can be addressed in the future:

- Different and potentially inconsistent state laws, if enacted could compromise the overall performance and utility of any solutions to address the gaps in this document.

- No standardization of practices and education for LEA to improve processes around reporting and monitoring stolen devices.
- Lack of full US carrier participation in the GSMA IMEI Database.
- There is a lack of information about the number of stolen smartphones that are shipped overseas.

2.4.4 Specification Sheet

2.4.4.1 Definition

Portal: Specially designed web page that brings information together from diverse sources in a uniform way.

2.4.4.2 Assumptions

1. Information provided by the Device Information Portal will not contain any personal information.
2. Information provided by the Device Information Portal will not contain any location information.
3. Information from industry sources will not be changed or altered.

2.4.4.3 Portal Platform

Central, credible entry point that brings together existing mobile device information from diverse industry sources (e.g., GSMA Database, OEM portals, other existing industry databases/sources).

1. The Device Information Portal provides the ability to query information about a mobile device (e.g., enrollment status, blacklist status) or direct users on how to determine device enrollment status.
2. The Device Information Portal becomes a vehicle to promote consumer awareness regarding mobile device theft prevention.
3. The Device Information Portal also provides anonymized statistics to the FCC Staff.

2.4.4.4 User Experience

1. Provides consolidated view of information from diverse sources in a uniform and easy to understand fashion.
2. Specific to IMEI and MEID to launch query.
3. Accessible from the Internet.
4. Publicly Accessible at no cost to consumers based on defined number of queries per day.
5. Law enforcement accessible at no cost to law enforcement (basic level of service).
6. Simple and easy to use UI (User Interface).
7. Available around the clock (24X7).

8. Limited to queries launched within the US (e.g., US IP Addresses).
9. Provides useful consumer advisories in the event of device loss or theft.
10. Provides Internet links to mobile device industry resources (e.g., Carrier website, OEM website).

3 On-Device Theft Prevention Features

3.1 Efforts Already in Progress

Mobile OS providers and manufacturers are currently delivering anti-theft features that typically combine on-device and remote functionality. As reported in Section 4.2 of the 2014 TAC MDTP report[5], solutions generally provide these basic features:

- On-Device passcodes and encryption of user data.
- Remotely Locate – get current location of the smartphone.
- Remotely Ring – ring or make noise even if the speaker is muted to help find smartphone.
- Remotely Disable Unauthorized Use of Essential Features – prevent access to information and apps on the smartphone through solutions like lock with PIN.
- Remotely Erase – remove user information from the smartphone.
- Enrollment Check – determine if a device is enrolled in an anti-theft solution.

The above basic features have been driven deep into the smartphone through the CTIA Smartphone Theft Voluntary Commitment and the laws subsequently passed in California and Minnesota as reported in Section 3.5 of the 2014 TAC MDTP report[5].

3.1.1 Existing Commitments and Laws

A comparison of the CTIA Smartphone Theft Voluntary Commitment and the law passed in California is highlighted below:

Table 3: Comparison of Anti-Theft Tools

Anti-Theft Tool:	CTIA Commitment	California Law (SB962)	Minnesota Law	Working Group View
Date: July 2015	Required	Required	Required	Required
Smartphones	Required	Required	Required	Required

[5] *Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP)*; Version 1.0; 1 December 2014; http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf.

Anti-Theft Tool:	CTIA Commitment	California Law (SB962)	Minnesota Law	Working Group View
No Cost to Consumer for devices sold at retail	Required	Silent	Required	Required
For retail sale, preloaded	Required if not Downloadable	Required if not Downloadable	Required if not Downloadable	Required if not downloadable with no additional purchase
For retail sale, downloadable	Required if not Preloaded	Required if not Downloadable	Required if not Preloaded	Required if not preloaded with no additional purchase
"shall include a technological solution at the time of sale"…….. "once initiated and successfully communicated to the smartphone" - SB962 Sec 2 (b) (1)	Required	Required	Required ("sold or purchased in MN" S.F. No. 1740, 2014)	Required
Remote Wipe	Required	Silent	Silent	Required
Allow the Authorized User to Render Essential Features Inoperable to Unauthorized Users Once Communicated	Required	Required	Silent	Required
Continue to function for 911 calls	Required	Not incompatible with 911	Silent	Required
Continue to function for emergency numbers programmed by the user.	Optional	Unclear	Silent	Optional
Prevent reactivation by unauthorized user including factory reset	Required to the extent technologically feasible	Required	Silent	Required to the extent technologically feasible
Restore user data to the extent feasible	Required	Silent	Silent	Required
Reverse inoperability if recovered by authorized user	Required	Required	Silent	Required
Initial Setup "prompt an authorized user to enable the technological solution" - SB962, Sec 2 (b) (1)	Silent	Required	Silent	Required
Opt-Out by Authorized User or Authorized User Designee, at any time SB962 Sec 2 (b) (2)	Silent	Required	Silent	Required
In addition, permit use of additional solutions if available - SB962 Sec 2 (3) (f)	Required, if available for users' smartphone	Allows, but does not require	Silent	Allowed but not required

Mobile OS providers and manufacturers are in various stages of deploying anti-theft solutions to comply with the voluntary commitments and state laws. California requires any smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, to include a technological solution at the time of sale, to be provided by the manufacturer or operating system provider, that, once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user.[6] The smartphone shall, during the initial device setup process, prompt an authorized user to enable the technological solution. In enacting SB 962, the California Legislature found that: "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."

3.1.2 Other Industry Activities

There are two types of anti-theft features. The first type is a passive "background feature" – like Reset Protection, Find My iPhone and Activation Lock, Reactivation Lock, on device passcode and encryption, etc. – that is enabled at initial device activation (or subsequently) by the authorized user. These background features place the device in a constant state of protection, without any additional user action regardless of theft/loss. The second set of anti-theft features are remote lock/erase and require additional user action after a device is lost or stolen in order to be triggered (e.g., going to a website to activate the action).

3.1.2.1 GSM Association Activities

Industry has invested significant resources and effort to develop mechanisms to help smartphone owners reduce the impact of smartphone theft and to assist their recovery if they fall victim. These mechanisms include the ability to disable operability of essential features on a stolen smartphone and to restore the smartphone to an operational state if it is returned to or found by its owner. The USA has led the world in seeking device based solutions and initiatives such at CTIA's Smartphone Anti-Theft Voluntary Commitment[7], and the introduction of legislative provisions in California and Minnesota have been particularly instrumental in facilitating and promoting the emergence of a range of anti-theft features.

GSMA, as a global trade organization, recognised the need to support the introduction of mechanisms that allow the remote disabling and restoration of essential features on a smartphone beyond the United States. Furthermore, GSMA's Device Security Group (DSG) recognised the need to mitigate the risk associated with the potential emergence of ad hoc, and potentially inconsistent requirements that might arise in the form of laws and regulations around the world. It has developed guidance for OS developers, device manufacturers, and other stakeholders to create a baseline set of features to deter smartphone theft worldwide. In seeking to address the fragmentation challenge GSMA developed guidance on features that have the potential to lead to the implementation of solutions that are widely supported by network operators, and device manufacturers.

---

[6] 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.

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

GSMA's work on defining feature guidance predates the establishment of the MDTP Working Group and the GSMA published its initial guidance in July 2014. That document defined a set of features that could be used by smartphone manufacturers, mobile network operators, and third party service providers, to assist in deterring smartphone theft, locating stolen smartphones, and protecting user data. These guidelines are intended to complement rather than replace network based device blocking.

The GSMA guidelines are focused on providing the following features for smartphones:

- Render essential features of the device inoperable.
- Prevent reactivation of the device unless by the owner or someone authorized by the owner.
- Wipe all user data.
- Allow the authorized user to re-enable their device and restore erased data that was stored to the cloud.
- Withstand hard reset.

These guidelines align with and build on the work already undertaken by CTIA and legislators, and leave the device manufacturers, mobile network operators, and third party service providers free to design specific offerings in a way that best suits their devices and businesses. The intention is to preserve the ability of the industry to innovate while aligning industry along a baseline set of anti-theft features.

Following publication of the first version of the feature guidance, GSMA refined and revised the guidance, and published an updated version of its "Anti-Theft Device Feature Requirements"[8] on 18th May 2015. GSMA is actively encouraging OS developers and device manufacturers to support the rollout of robust anti-theft features for the protection and benefit of device owners. GSMA also urges other stakeholders to allow industry to innovate in a manner unencumbered by the unnecessary introduction of restrictive regulatory or legal provisions.

3.1.2.2 ITU Activities

ITU-T Study Group 17, which has responsibility for security matters within the ITU-T, formally approved and established a work item in September 2014 to define "Functional Security Requirements and Architecture for Mobile Phone Anti-theft Measures"[9].

The scope of the planned work will extend beyond existing legislative and voluntary industry initiatives in the USA and elsewhere, and is designed to result in a formal ITU-T Recommendation. The stated aim is to take existing work and define the security requirements and architecture that providers of smartphone based solutions must satisfy and to include these in Supplement 19 to ITU-T X-series Recommendations (2013) on security aspects of smartphones.

This work, which is in its infancy, is supported by Brazil, China, Republic of Korea, Sudan, and Uganda. GSMA and 3GPP have been invited to collaborate but the GSMA is not supportive of

[8] http://www.gsma.com/newsroom/all-documents/sg-24-anti-theft-device-feature-requirements-v2-0/
[9] http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10278

such descriptive work being undertaken by standards development organizations. The work is well intentioned and is worthy of being monitored.

3.1.2.3 ATIS Activities

In support of the industry efforts related to mobile device theft prevention and to address the need of Law Enforcement to obtain IMEI information from mobile devices, ATIS undertook a work item in 2015 to develop a best practices specification for obtaining the IMEI from locked and unlocked mobile devices. In October 2015, ATIS published ATIS-07-0700024 "Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)" which is available at https://access.atis.org/apps/group_public/download.php/25150/ATIS-0700024.pdf.

3.2 Topics for Future MDTP Working Group Discussions

The following points are intended as constructive and proactive options for the group to consider as next discussion topics for the MDTP Working Group.

- Centralized data gathering post July 2015 (e.g., through CTIA with input from OS providers, mobile operators, and law enforcement agencies, where applicable) on consumer adoption rates of background anti-theft features in light of the California requirement (effective in July 2015) to prompt users to enable the feature at initial device setup. Data gathering also could include follow-up on consumer awareness/understanding, smartphone theft rates and, to the extent possible, rich data on time/location/circumstances surrounding smartphone theft. At least one years' worth of data would be helpful, as this will include new devices purchased in the holiday buying season and provide sufficient time for consumers to develop familiarity with the features.
    - Set up the common framework for collection of the data and framework for analysis of the data.
    - Smartphone assumed. WiFi only devices not addressed.
- Enhanced consumer outreach and education – For example, we could contribute to a tutorial on anti-theft features of the different mobile operating systems that lives on www.fcc.gov and individual manufacturers' and operators' web sites could link to that or develop their own if they don't already have one. Could also include information and guidelines around what to do if your phone is stolen (e.g., remote lock your phone, erase data, call your mobile operator, report to police, etc.).
- Reporting for Law Enforcement – Using the mechanisms being developed in ATIS and GSMA on enabling a mechanism for IMEI to be retrieved on disabled devices and educational outreach to law enforcement on using the mechanism.
- Increased consumer adoption of anti-theft features – For example, some mobile operating systems recommend or encourage end users during device setup to enable anti-theft features. Currently, the laws prompt the user to choose to turn these features on, but we could highlight the additional steps that some are taking to encourage enablement, not as a prescription for others to adopt, but to illustrate the good faith efforts of the industry here.

3.3 How to Increase Consumer Use of These Functions

Many devices currently in-market do not have background anti-theft features, thus customer enablement is not currently available across the array of smartphones in the marketplace. The background anti-theft features are expected to be available on all new smartphones come July. Under the California law, users must be prompted during initial device setup process to activate the feature, which should be a powerful driver of enablement. Even before widespread availability of background anti-theft features, there is empirical evidence that consumers are increasing usage of anti-theft features on smartphones[10]. Unfortunately, we do not, at this time, have sufficient data to determine what has led to the increase in consumer usage of anti-theft features. The MDTP Working Group recommends a deeper investigation by industry into the causal factors for the increase in consumer use of these functions that could be used for determining how to optimize further efforts to incentivize greater consumer use of anti-theft features, if necessary.

In addition, the availability of anti-theft features on all smartphones is expected to increase by the effective date of the CTIA Voluntary Commitment, and the California and Minnesota laws. Under the California law, users must be prompted during initial device setup process to activate theft deterrent features. The MDTP Working Group recommends an industry-led investigation into whether the increased availability of anti-theft functionality on new smartphones as well as the upcoming initial device setup prompts that will be required by California legislation after July 2015 have the effect of further increasing consumer use of these features. Such a study should be undertaken sufficiently after the July 1, 2015 date to allow for a sufficient number of devices with these features to have been placed into circulation.

Analyzing trends in consumer usage and obtaining an empirical understanding of consumer usage patterns will provide a data-driven basis for determining whether any further action is needed to increase customer usage of anti-theft features and, if so, provide a clear understanding of factors that either encourage or discourage consumer use. In doing so, remedial efforts can be targeted to resolve empirically identified obstacles.

4 Considerations for Hardening IMEI and Additional Device Identifiers

4.1 Introduction

Although the problem of device theft is not of the industry's creation, a range of stakeholders recognize device theft as being a major public policy concern and the need to reduce the attractiveness of stolen mobile devices by preventing their reuse after a theft. To that end, mobile network operators have the ability to block specific devices from accessing their networks. This functionality was originally created to block devices that were not approved or could cause interference on mobile networks and can now be used to take action against stolen devices.

To control network access, operators can create databases within their networks in which the electronic identities of devices can be stored. Devices to be disabled can then be registered on a "blacklist". During the registration and authentication process that occurs whenever a device

[10] http://www.ctia.org/resource-library/press-releases/archive/more-americans-use-pins-and-passwords-to-protect-personal-data

attempts to connect to a mobile network the identity of that device is checked against the database and if it is contained in the blacklist, access will be denied.

Despite the need for mobile devices to have secure unique identities that cannot changed some devices had back doors designed in so that the identities could be easily changed for servicing reasons. Unfortunately, these back doors were discovered and exploited by unauthorized parties, and this has resulted in identities being tampered with and network operators have reported the presence of devices on their networks with duplicated and invalid identities. This circumvention of the requirement that identities should not be capable of being changed outside the control of the original device manufacturer has the potential to undermine the efficacy of network blocking of stolen devices.

4.2 Device Identity Security

The effectiveness of device blocking on mobile networks is dependent on the secure implementation of device identities. Therefore, although network blocking does not represent the final solution to device theft, it is essential that it is complemented by the efforts of the device manufacturing community to ensure that devices delivered to market incorporate appropriate security features. Enhanced device identity integrity is essential to the efficient and effective network blocking of stolen mobile devices.

Although the mobile standards require that device identities should not be capable of being changed after the point of manufacture it became apparent over a number of years that identities were being changed with relative ease. This had the effect of jeopardizing industry efforts to combat device theft as identities could be changed on stolen devices from the original identities that had been blocked thereby bypassing the action taken by network operators. That necessitated a concerted industry effort to consider what could be done to improve the mobile device security landscape. Significant efforts were made to improve the situation with real commitment and engagement by the device manufacturing community, and these led to a series of initiatives that have been central to improved device identity security levels.

4.3 Device Identity Standards

Mobile technology standards provide that mobile identities must be unique per device and that they must be protected against alteration after the point of manufacture. However, no details or guidance are provided as to how exactly these security goals are to be achieved, and industry considered the suitability of the standards to define how device identities should be secured.

Following detailed analysis, industry concluded that standardization is unsuitable as a means to deal with device identity issues and that incorporating enhanced security features in the standards could be problematic and undesirable. Industry consensus was that standardization would confer no benefit and had the potential to do more harm than good based in the following conclusions:

- Standardizing the technical means to protect device identities could expose devices to even greater risk if the prescribed safeguards are compromised as that would expose all devices if one method fits all.
- Currently, OEMs and chipset suppliers have different security implementations, some better than others, but mandating a single solution would most likely remove the enhanced level of protection offered by some manufacturers.

- The work to standardize a single solution, or even a small range of solutions, would be very difficult as every manufacturer would want their specific approaches to be adopted and that is unlikely to result in any consensus and could ultimately result in a race to the bottom to satisfy the ability of the less innovative manufacturers.
- By definition, standards are publicly available and describing how device identities are secured in mobile devices is likely to be welcomed by the hacker community but not likely to increase the security of the implementations.
- Standardizing device identity security measures could stifle innovation and would be unlikely to take into account new and evolving attacks to which a standards based response could be difficult, inflexible and slow.
- The usefulness of standards to deal with security matters is questionable as standards are optional and defining mandatory features in voluntary standards does not constitute a credible solution. This is evidenced by the fact that the standards already mandate that device identities must be non-reprogrammable after the point of manufacture but this hasn't solved the problem. Adding more detail in terms of how this should be done is unlikely to yield better results.
- Investing in and improving device identity security should be undertaken in the context of a broad/er industry effort to secure devices and develop anti-theft measures, and these typically sit outside the standardization domain.

The ultimate conclusion was that mandating a single mechanism by which device identities should be protected is undesirable. Industry defined design principles, that would be reviewed and updated as needed, and a market surveillance and issue resolution process to monitor compliance were considered preferable.

4.4 Device Identity Security Initiatives

As an alternative to standardization, the GSM Association led the development of two major industry initiatives designed to enhance the security of mobile device identity implementations. The two initiatives that were initially launched in 2005 are described below.

4.4.1 Technical Design Principles

Although the standards mandate that device identities should not be changeable, the specifications do not indicate any details on implementation characteristics. In order not to stifle innovation, industry resisted the temptation to standardize how to secure device identities whilst recognizing the benefit of setting out high level security design principles.

This initiative, and the level of detail it entailed, represented a significant improvement on the existing specifications and the industry agreed nine principles provided guidance to device manufacturers, and provided network operators and other wholesale device purchasers with a set of criteria against which device security could be assessed and compared.

1. Secure uploading, downloading, and storage of executable code and sensitive data related to the IMEI implementation.

2. Protection of components' executable code and sensitive data related to the IMEI implementation.
3. Protection against exchange of data/software between devices.
4. Protection of executable code and sensitive data related to the IMEI implementation from external attacks.
5. Prevention of download of a previous software version.
6. Detection of, and response to, unauthorized tampering.
7. Software quality measures.
8. Hidden menus should not have the ability to access or modify executable code or sensitive data.
9. Prevention of substitution of hardware components.

These principles help device manufactures to develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which the device identity is stored.

4.4.2 IMEI Security Weakness Reporting and Correction Process

It is acknowledged that security is not absolute and despite the best efforts of device manufacturers it is possible that once secure device identity implementations may be compromised at a later stage. Consequently, GSMA and the world's leading mobile device manufacturers established a formal process to centralize the reporting and correction of newly identified device identity security weaknesses to improve device security levels during the manufacturing life cycle of current and future device products. GSMA acts as a central clearing house for reports on device models that are believed to have had their identity security compromised. These reports are referred to the relevant manufacturers, investigated, and responded to within 42 days. The reports contain details of proposed remedial action and dates from which equipment with new security measures will be introduced.

The overall objective of this initiative is to improve handset security levels during the manufacturing life cycle of current and future products, and improved communications greatly enhances the exchange of intelligence, and accelerates co-operation between the manufacturer and network operator communities. The reporting process engages with manufacturers and the operator community centrally rather than locally to ensure that there is increased awareness and visibility of any problems that arise.

4.5 Current Situation

The commitment of the world's leading device manufacturers to the GSMA led initiatives was encouraging and 21 of the largest device manufacturers formally signed up to support both initiatives. The support of such a critical mass of device manufacturers was critical and constituted an early indicator that the technical principles, and the reporting and correction process would have a positive impact on device identity security which would help increase confidence in the effectiveness of network blocking of stolen devices.

GSMA undertook to periodically review the effectiveness of the voluntary industry initiatives to measure success and to propose any enhancements that may be deemed appropriate and beneficial. A comprehensive review was undertaken in 2011 and it noted that significant progress had been made by most device manufacturers in increasing device identity security levels with the result that IMEI reprogramming was no longer prevalent. The number of devices with vulnerable identities had decreased by 77%, the number of manufacturers with vulnerable products reduced by 45% from 11 to 6 and the number of available and effective hacking tools had shown a 72% decrease. Problems did persist with two manufacturers that, between them, accounted for 83% of compromised device models and their failure to respond appropriately to reported security problems was regrettable.

The improvements in identity security noted in 2011 resulted in the termination of a GSMA funded monitoring service in 2012 which had been running for a number of years. Since then no detailed statistics have been available to illustrate the extent or nature of device identity changing but anecdotal evidence suggests that device identities have come under sustained attack from embedded systems hackers whose expertise has grown over time. Statistics presented to GSMA's Device Security Group in July 2015 that covered 2013 and 2014 suggested that the number of compromised models is at least on a par with 2011 suggesting little or no improvement since then, at least by some manufacturers.

Modification of device identities is a criminal offence in some jurisdictions but not in the United States where websites and outlets exist and are on the increase that openly advertise the ability to change device identities. Developers of attacks against device identities are known to the based in the USA, Israel, India, and Eastern Europe. Legislation to criminalize unauthorized device identity reprogramming, and enforcement of it and prosecution of offenders, could help reduce the attractiveness of this activity and the attendant problem of device identity changing.

5 Recommendations

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

- Actionable Recommendations
- Areas for Future Consideration

5.1 Actionable Recommendations

Recommendation 1.1: The FCC TAC recommends that the CTIA – The Wireless Association and the GSMA, on behalf of the industry, implement the Device Information Portal based on the objectives contained is Section 2.4 of the TAC MDTP Analysis and Recommendations Report for 2015.

Recommendation 1.2: The FCC TAC recommends that the CTIA-The Wireless Association to update their ongoing study and research on consumer usage and trends for smartphone security prior to July 2016. In particular, the study should aim to determine whether uptake for anti-theft features continues to improve once the features are available across all new smartphone models that make their way into consumers' hands. The study should also analyze adoption rates among the respondents.

Recommendation 1.3: The FCC TAC recommends that the FCC work with industry on developing effective outreach initiatives to educate the consumer. An example is to create a website/consumer education portal and outreach program that informs users about the anti-theft initiatives and legislation industry is committing to support, and link to each of the smartphone manufacturers' webpages that describe their anti-theft features.

Recommendation 1.4: The FCC TAC recommends a deeper investigation by industry into the causal factors for the increase in consumer use of MDTP functions that could be used for determining how to optimize further efforts to incentivize greater consumer use of anti-theft features, if necessary.

Recommendation 1.5: The FCC TAC recommends an industry-led investigation into whether the increased availability of anti-theft functionality on new smartphones as well as the upcoming initial device setup prompts that will be required by California legislation after July 2015 have any effect including increasing consumer use of these features. Such a study should be undertaken sufficiently after the July 1, 2015 date to allow for a sufficient number of devices with these features to have been placed into circulation.

Recommendation 1.6: The FCC TAC recommends ATIS, working with other key stakeholders such as the GSM Association, identify key technological areas where the FCC should seek further information from industry, including:

1. IMEI
2. Requirements and use of databases
3. Future theft prevention opportunities

Recommendation 1.7: The FCC TAC recommends industry adoption of the voluntary framework for a set of on-device capabilities to guide industry based on the "working group view" column of the Table 3: Comparison of Anti-Theft Tools in Section 3.1.1 Existing Commitments and Laws. CTIA should maintain a publicly available list of OEMs/OS Providers/Carriers reflecting the CTIA Smartphone Voluntary Commitment and voluntarily support of the "working group view" column of Table 3.

Recommendation 1.8: The FCC TAC recommends the GSMA's North American Regional Interest Group, with support from the GSM Association, develop a Best Practices/ Implementation Guideline for device blacklisting, device blocking, and data sharing.

Recommendation 1.9: The FCC TAC recommends that GSMA, working with the mobile device manufacturing community and other stakeholders (e.g., CTIA), review the 2005 published technical design principles[11] and security weakness reporting and correction process[12] to ensure they take into account current threats and attack scenarios and remain fit for purpose and that GSMA invite the manufacturers to reconfirm their support for these initiatives.

Recommendation 1.10: The FCC TAC recommends that the GSMA and CTIA coordinate a survey of the US carriers to assess and measure the extent to which invalid and duplicate device identities may be in use on their networks.

---

[11] 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

[12] IMEI Weakness Reporting and Correction Process - http://www.gsma.com/publicpolicy/wp-content/uploads/2007/07/IMEI-Weakness-Reporting-and-Correction-Process-3.2.0.pdf

Recommendation 1.11: The FCC TAC recommends that the industry reinstate a service to monitor for and report security issues to provide statistical data and to ensure identified problems are notified to the affected device manufacturers.

Recommendation 1.12: The FCC TAC recommends that the FCC work with Congress on the enactment of legislation to criminalize the unauthorized changing of device identities and to supply or possess equipment to undertake the unauthorized changing of device identities. The proposed legislation should be enforced and offenders prosecuted as a disincentive to engaging in the unauthorized changing of device identities.

Recommendation 1.13: The FCC TAC encourages the FCC to facilitate the convening of Operational Law enforcement subject matter experts to discuss mobile device theft with regard to response, outreach, education, prevention, tactics, best practices, tools, analytics, and collaboration across jurisdictions.

5.2 Areas for Future Consideration

Recommendation 2.1: The FCC TAC recommends the FCC TAC/MDTP Working Group consider study on discussion topics in Section 3.2 regarding centralized data gathering, enhanced consumer outreach and education, reporting for law enforcement, and increased consumer adoption of anti-theft features.

Recommendation 2.2: The FCC TAC recommends the FCC TAC/MDTP Working Group consider study on how to expand blacklisting to all US carriers, working with the GSM Association and CTIA.

Recommendation 2.3: The FCC TAC recommends the FCC TAC/MDTP Working Group should examine if anti-theft solution providers may be able to provide consumers a feature to determine enrollment status in their solution in such a way that the consumer does not have to be in physical possession of the device.

Note: The following are the links to the CTIA website for theft protection tools:

Android:

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

http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-for-android-wireless-handsets---page-2

iOS:

http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-for-ios-apple-wireless-handsets

Blackberry:

http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-for-blackberry

Windows:

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

Recommendation 2.4: The FCC TAC recommends the FCC TAC MDTP Working Group should continue studies to determine whether implementations post July 2015 have the desired effect on mobile device theft. This recommendation refers to the planned recurring survey effort for continued monitoring of improvements, and to set up the common framework for collection of centralized data post July 2015 (e.g., through CTIA with input from OS providers, mobile operators, and law enforcement agencies) and framework for analysis of the data. Methods for better tracking of actual phones stolen should also be investigated.

Appendix A: Glossary

CDR	**Call Detail Record**
CS	**Circuit Switched**
EIR	**Equipment Identity Register**
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.
GSMA	**GSM Association**
GSMA-NA	**GSM Association North America Regional Interest Group**
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 by a cellular 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).
LTE	**Long Term Evolution**
MDTP	**Mobile Device Theft Prevention**
MIN	**Mobile Identification Number** The MIN, more commonly known as a cellular phone number, uniquely identifies a mobile device that is paired with a cellular wireless network. The MIN is dialed from other cellular 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.
MSISDN	**Mobile Station Integrated Services Digital Network**
PS	Packet Switched

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.)

Appendix B: Information Aggregator Database Solutions

B.1 Recipero Solution

Recipero provides a database to track the status of mobile devices consisting of an eco-system of multiple contributors, all of whom have a vested interest in making sure that the information is accurate and readily available. This allows the system to address multiple types of theft and fraud over and above consumer theft. The ecosystem consists of Cellular Carriers, Insurance Companies, Traders, Recyclers, Retailers, Law Enforcement Agencies, and Consumers.

Recipero is the largest data aggregator of lost and stolen data, and other data that indicates if a mobile device has been compromised for resale. Recipero receives data from the cellular carriers directly, the GSMA database, mobile insurance companies, rental and finance companies, consumers, and the FBI's NCIC database. Recipero also tracks trading activity from thousands of traders and recyclers. Our solution ensures our customers aren't accepting trade-ins that have been reported lost or stolen, and gives consumers peace of mind that the phone they are purchasing is not compromised for their use when they are buying phones in the second hand market. Recipero believes that these "second victims of crime" need to be protected as well.

Recipero can also monitor phones that are on finance contracts. When a customer attempts to sell a device, Recipero can immediately alert the carrier, or retailer that their customer is trying to trade a device. This allows their customer care to conduct an outreach call to the customer to determine if they can save the customer and facilitate a trade in, or upgrade for that customer.

Additionally, Recipero has the ability to monitor devices from the time they come into the supply chain and are sent to retail stores to give retailers and carriers instant notification if someone steals a phone/phones from inventory and tries to sell the phone/phones in the open market. This allows the risk management teams to begin their investigation at the time of theft vs. at the end of the month when inventory is done and they see there has been shrinkage at a store, or in the supply chain. Recipero also flag the phones as red to the traders so they will not accept the devices.

B.2 GSMA Device Check

GSMA Device Check enables insurers, recyclers, mobile network operators and law enforcement agencies to identify suspect devices, minimize loss and combat crime. GSMA Device Check is a real-time service that provides access to GSMA's IMEI/MEID Database, the world's most comprehensive and which is a direct source of International Mobile Equipment Identifier (IMEI) data indicating device model and lost or stolen status. With this easy-to-use service a range of stakeholders, insurers and recyclers can accurately and confidently process claims, or execute recycling transactions or simply run checks on the lost/stolen status of a device with confidence. Use of the Device Check service is widespread across a number of diverse stakeholder groups and sectors, some of which are described below.

B.2.1 Public Look Device Checking

GSMA supports public device look up services in multiple countries and is capable of providing a direct public look up service itself. The public look up services provide the device blacklist status, device make and model details, and access can be limited to a specific region or country.

GSMA captures checking history events which are available to law enforcement agencies on request.

B.2.2 Law Enforcement Device Checking

GSMA supports law enforcement blacklist look up services in multiple countries. These services allow officers to check the status of a device as well as the checking history of individual devices. A blacklist indication enables officers to carry out their investigations, indicate the likelihood of a crime having been committed and impound stolen devices. When a crime is reported to law enforcement but the device identity has not been blacklisted that could be an indicator of intent to commit a future fraud by the individual making the crime report. The checking history pertaining to a device enables officers to identify which dealer or retailor a device has been presented to in order to follow up on crime investigations.

B.2.3 Retail and Dealer Device Checking

GSMA is a leading provider of retail and trader device checking services in the USA and other countries. The users may check the status of a device presented for trading or recycling to identify and screen out stolen goods. GSMA captures checking history events which are made available to law enforcement agencies.

B.2.4 Insurance Checking

GSMA provides a device checking service to insurers enabling them to confirm the status of a device and whether a device has been blocked prior to paying out an insurance claim. Absence of blacklisting may indicate a fraudulent claim attempt. GSMA captures checking history events which are available to law enforcement systems.

B.2.5 Aggregator Support

GSMA supports aggregators with access to the IMEI/MEID Database under controlled conditions and in accordance with policies defined by GSMA members pertaining to database and data access.

B.2.6 Customs and Excise

GSMA provides device identity information to customs organizations internationally for the screening and verification of device imports.

Applicants for look-up access to GSMA Device Check must demonstrate they are mobile insurers, device recyclers, authorized dealers, repair centers, law enforcement agencies, regulatory bodies, or associated national interest groups.

B.3 iconectiv Device Registry

iconectiv, a wholly owned / independent subsidiary of Ericsson d.b.a. Telcordia, develops market-leading solutions that enable operators to interconnect networks, devices, and

applications critical to evolving the global telecommunications marketplace. Originally Bell Core (1984) then Telcordia and now iconectiv, the company has 31 years of expertise in delivering software solutions to the telecom industry in the US and overseas.

Powerful, trusted, and neutral solutions for the telecommunications industry include number portability solutions (19 countries worldwide), mobile messaging services, anti-theft mobile device registries, spectrum management databases and other interconnection information services. iconectiv solutions are used by more than 1,000 operators, regulators and content providers and are currently used to provide services to over a billion end users.

Recent key initiatives include Common Short Code Administration (CSCA) and the NPAC (Number Portability Administration Center).

The iconectiv Device Registry is a next generation centralized registry of mobile device data. Device Registry combines device information from Operator networks, government and other third-parties, cross-referencing them with the national number portability database and device blacklist databases. It includes capabilities for automatically collecting critical device data from the network such as IMEI, IMSI, and MSISDN to build a unique mobile fingerprint, and analytics to detect and block cloning and IMEI reprogramming. It protects consumers and enterprise users from mobile device theft and minimizes the use of black market and counterfeit devices, thus stopping the leakage of import and tax revenues.

For further information, please see: http://www.iconectiv.com/anti-theft/device-registry/index.html.