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

Version 1.0

<date>

Table of Contents

Executive Summary

Editor's Note 3/17/16: Executive Summary to be developed when majority of the body of this report is complete and stable.

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 2015. The work proposed for 2016 includes developing recommendations on:

- Next generation anti-theft features;
- Assessment of the effect of previous recommendations on device theft;
- Development of recommendations for improvements in consumer outreach efforts;
- Development of mechanisms to support easier access for law enforcement to IMEI information;
- Examination of methods for carriers to provide more useful data related to device theft and for fostering greater global effectiveness of proposed solutions.

1.3 Scope of Work

The scope of this report is to provide an evaluation of the industry mobile device theft prevention activities based upon the recommendations of the 2014 and 2015 reports of the FCC TAC Mobile Device Theft Prevention Working Group.

1.4 Methodology

Editor's Note 3/17/16: The Methodology section is to be written.

1.5 MDTP Working Group Membership

Table 1.1: MDTP Working Group Membership

Name	Organization
Brian K. Daly, Co-Chair	AT&T
Robert Kubik, Co-Chair	Samsung
Ogechi Anaytonwu	Asurion
Jay Barbour	Blackberry
Bradley Blanken	Competitive Carriers Association (CCA)
Craig Boswell	Hobi
Mike Carson	ebay
David Dillard	Recipero
Chris Drake	iconectiv
Eric Feldman	ICE/Homeland Security Investigations
Thomas Fitzgerald	New York City Police Department
Les Gray	Recipero
Gunnar Halley	Microsoft
Joseph Hansen	Motorola Mobility
Mark Harmon	Recipero
Jamie Hastings	CTIA
Joseph Heaps	Department of Justice (DOJ), National Institute of Justice
Gary Jones	T-Mobile USA
Sang Kim	LG
John Marinho	CTIA
Jack Mcartney	Recipero
Samuel Messinger	US Secret Service
James Moran	GSM Association
Jason Novak	Apple
Kirthika Parmeswaran	iconectiv
Greg Post	Recipero
Timothy Powderly	Apple

Name	Organization
Dennis Roberson (TAC Chair)	Illinois Institute of Technology
Matt Rowe	Gazelle
Christian Schorle	FBI
David Strumwasser	Verizon Wireless
Maxwell Szabo	City and County of San Francisco
Samir Vaidya	Verizon Wireless

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

- 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 contains the MDTP recommendations for industry from the 2014 MDTP report and the 2015 MDTP report.
- Section 3 describes the industry MDTP related activities.
- Section 4 provides the cross referencing between the recommendations and the industry activities.
- Section 5 identifies any gaps in the industry MDTP activities.
- Section 6 contains the MDTP recommendations for 2016.
- Section 7 contains the report conclusions.
- Appendix A is the Glossary.

2 MDTP Recommendations for Industry from 2014 and 2015

This section contains the recommendations from the 2014 and the 2015 which are applicable to industry activities. Only the recommendations for the 2014 and 2015 reports which are related to industry activities have been included in this 2016 report.

Note: In the descriptions of some of the recommendations, there are references to tables and sections. These references are to the tables and sections of the respective 2014 and 2015 MDTP reports and not to the tables and sections of this report.

The recommendations are quoted in this report exactly as this appeared in the 2014 and 2015 MDTP reports with one small modification. In order to know the associated report of each recommendation, the recommendation number has been modified to add either (2014) or (2015) as a prefix to the Recommendation number. For example, **Recommendation x.y** from the 2014 report is written as **Recommendation (2014) x.y**.

The following Recommendations from the 2014 MDTP report are not related to industry activities and have been excluded from this report:

- 2014 Recommendation 1.1
- 2014 Recommendation 1.2
- 2014 Recommendation 1.3
- 2014 Recommendation 1.8
- 2014 Recommendation 1.9
- 2014 Recommendation 1.10
- 2014 Recommendation 1.11
- 2014 Recommendation 1.12
- 2014 Recommendation 1.13
- 2014 Recommendation 1.14
- 2014 Recommendation 1.17
- 2014 Recommendation 1.18
- 2014 Recommendation 2.1

The following Recommendations from the 2015 MDTP report are not related to industry activities and have been excluded from this report:

- 2015 Recommendation 1.12
- 2015 Recommendation 1.13

2.1 2014 MDTP Recommendations for Industry

The following are MDTP recommendation for industry as quoted in the 2014 MDTP working group report:

> ***Recommendation (2014) 1.4:*** *The FCC TAC recommends that CSRIC, in coordination with appropriate industry standards bodies (e.g., GSMA-NA Regional Interest Group, ATIS), be tasked with developing policies, methods or procedures for law enforcement to obtain device identifiers from smartphones in their possession that are under theft investigation.*
>
> ***Recommendation (2014) 1.5:*** *The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.*
>
> > *Note: Device identifiers are typically available on smartphones either through a label on the device (which may be under the back cover or under the battery), or available through a menu option on the screen. This recommendation is to define standards, methods, and procedures for obtaining such identifiers from the device even if the device is locked or disabled, and may include a combination of physical and electronic methods for obtaining the identifier.*
>
> ***Recommendation (2014) 1.6:*** *The FCC TAC recommends that CTIA convene a joint Law Enforcement, carrier, and wireless industry task force to define a consumer outreach process to encourage consumers to initially report smartphone thefts to their carrier.*

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

Recommendation (2014) 1.7: *The FCC TAC recommends that the FCC TAC/MDTP Working Group continue the joint task force between key theft reporting points such as carriers, insurers, law enforcement, and other relevant industry reporting points to define a process for the capture of comprehensive data (e.g., number stolen, make, model, distribution, device trail) relative to smartphone thefts and encourage increased data sharing to ensure up-to-date information and timely visibility of reported theft events. The FCC should encourage greater use of the existing device registry databases.*

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

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

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

Recommendation (2014) 1.15: *The FCC TAC recommends that the FCC work with CTIA and GSMA's North American Regional Interest Group to encourage additional operators to participate in the April 10, 2012 voluntary commitment[1] to take certain actions (e.g., GSMA IMEI Database) to help law enforcement deter smartphone theft and protect personal data. This voluntary commitment includes the technology aspect of operators using the GSMA IMEI Database or CDMA database to blacklist devices reported stolen, and then using those blacklists across operators to deny service on the network using network-based technology solutions such as an Equipment Identity Register or other fraud prevention systems available on carrier networks.*

Recommendation (2014) 2.1: *The FCC TAC recommends that a single law enforcement point of contact be established to serve as a clearinghouse of information and expertise on mobile device theft, much like the National Mobile Phone Crime Unit in the United Kingdom.*

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

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

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

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

Recommendation (2014) 2.2: *The FCC TAC recommends that an education campaign be developed with the assistance of the GSMA-NA Regional Interest Group and CTIA and coordinated with law enforcement associations for dissemination to police officers to educate them on important aspects relative to smartphone theft.*

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

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

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

Recommendation (2014) 3.1: *The FCC TAC recommends that CTIA convene an ongoing study of how to make anti-theft solutions easy for consumers to understand and use, potentially providing consistent messaging on next steps when theft occurs.*

Recommendation (2014) 3.2: *The FCC TAC recommends that solutions providers and the ecosystem involved in reverse logistics (carriers, device recyclers, device resellers, etc.) ensure that the solution providers have enacted a mechanism for reverse logistics providers. The approaches to such mechanisms vary by solution provider, but as long as there are manual or automated means to successfully achieve disabling protection, industry stakeholders should have flexibility in determining the right approach. A prescriptive recommendation on the technical approach to reverse logistics limits innovation by solution providers in a competitive market.*

Recommendation (2014) 3.3: *The FCC recommends that CTIA convene a joint Law Enforcement, carrier, and wireless industry task force, in cooperation with consumer groups (e.g., Consumers Union), to define a process for law enforcement to repatriate a stolen smartphone if found or recovered.*

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

Recommendation (2014) 3.4: *The FCC recommends that CTIA in coordination with the carriers and wireless industry develop a method and procedure for consumers to be able to lookup smartphone IMEI/MEID status.*

Note: This is similar to what is available on the Canadian web site[2].

Recommendation (2014) 3.5: *The FCC TAC recommends that smartphone anti-theft solution providers offer a mechanism for consumers to check enrollment status of a device in the solution.*

Recommendation (2014) 3.6: *The FCC TAC recommends that the industry continue its work educating consumers about how they can protect their data and their smartphones to augment what the FCC and law enforcement is doing.*

Recommendation (2014) 3.7: *The FCC TAC recommends that the industry continue to share its best practices with the FCC and work with the FCC as needed on the consumer outreach program.*

Recommendation (2014) 3.8: *The FCC TAC recommends that the GSM Association's North American Regional Interest Group and CTIA jointly develop a voluntary process to report to the FCC statistics on devices reported lost or stolen over a 12 month period, using the CWTA report to the Canadian Radio-television and Telecommunications Commission as a model.*

Recommendation (2014) 3.9: *The FCC TAC recommends that the GSM Association's North American Regional Interest Group, along with other appropriate stakeholders, develop a best practices and guidelines on how to measure and report on blacklisted devices going forward, including guidelines to establish consensus in terms of blacklisting policies to ensure consistency of what is blocked and measured.*

Recommendation (2014) 4.1: *The FCC TAC recommends the FCC TAC/MDTP Working Group perform ongoing study of potential new, measurable risks to public safety that requires future assessment and consideration by industry.*

Recommendation (2014) 4.2: *The FCC TAC recommends the industry TAC/MDTP Working Group perform ongoing study and monitoring of the dynamic and changing threat environment.*

Recommendation (2014) 4.3: *The FCC TAC recommends the FCC TAC/MDTP Working Group perform ongoing study and consideration of new and emerging technologies and global standards for the purpose of aiding in the mitigation of smartphone theft.*

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

Recommendation (2014) 4.4: *The FCC, working with the FCC TAC/MDTP Working Group, should provide an annual assessment of smartphone theft and assess the effectiveness of the measures undertaken to combat theft. In addition, the FCC should assess the effectiveness of tools provided to law enforcement including the rate of participation in law enforcement in using such tools.*

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

2.2 2015 MDTP Recommendations for Industry

The following are MDTP recommendation for industry as quoted in the 2015 MDTP working group report:

> ***Recommendation (2015) 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 (2015) 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 (2015) 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 (2015) 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 (2015) 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 (2015) 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 (2015) 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 (2015) 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 (2015) 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[3] and security weakness reporting and correction process[4] 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 (2015) 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.*

Recommendation (2015) 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 (2015) 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 (2015) 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 (2015) 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

[3] 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

[4] 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

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 (2015) 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.*

3 Industry MDTP Related Activities

This section describes the various MDTP related activities of the industry. These activities have been organized into sections for ATIS, CTIA, and GSMA based upon the associated lead or primary organization for the specific industry activity.

3.1 ATIS MTDP Related Activities

Editor's Note 3/17/16: This section is to be expanded with additional ATIS MDTP related activities.

3.1.1 ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

In October 2015, ATIS published the specification ATIS-0700024 "Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)".[5] This specification provides best practices for the following scenarios:

- Device Disabled By Owner Initiated MDTP Procedures
- IMEI Display on Disabled or Locked Devices
- IMEI Display on Unlocked Devices

3.2 CTIA MDTP Related Activities

3.2.1 CTIA Mobile Device Information Portal (MDIP)

Based on the efforts and recommendations of the TAC MDTP Working Group, in February 2016 CTIA issued a publicly available Request for Proposal (RFP) for the implementation of a Mobile Device Information Portal (MDIP). Per the RFP, responses to the RFP were due in March 2016 the MDIP will be available to consumers, law enforcement and commercial entities to enable checking of IMEI and MEID information with respect to placement on the industry Black List. The MDIP is envisioned to be available by the end of 2016 for the Phase 1 set of requirements as described in the RFP. Phase two requirements are envisioned for implementation in 2017.

3.2.2 CTIA Stolen Phones Working Group

The CTIA Stolen Phones Working Group (SPWG) was established as the group to address industry response to the recommendation of the TAC MDTP Working Group. The SPWG worked with industry to put in place the Anti-Theft Voluntary Commitment and also the implementation of the MDIP. The SPWG is also the point for coordination with GSMA and GSMA-NA regarding industry best practices and outreach to law enforcement and other relevant industry stakeholders.

3.2.3 CTIA Annual Survey of Consumers

Based on the request by FCC Staff and the TAC MDTP Working Group, CTIA committed to conduct an annual survey of consumers to solicit information regarding the adoption of anti-theft security tools on smartphones. Previous released survey results by CTIA indicated significant improvement in adoption rates over the period 2012 to 2015. A recent survey was conducted during the first quarter of 2016 by CTIA and results have been compiled in order to share the information with the TAC MDTP Working Group. The results continue to show improved consumer adoption rates as it relates to the adoption of anti-theft security features on smartphones.

[5] Available as a public download from ATIS at https://access.atis.org/apps/group_public/download.php/25150/ATIS-0700024.pdf .

3.2.4 CTIA Survey of Carriers

Based on the recommendations of the TAC MDTP Working Group, CTIA undertook an anonymized survey of carriers across the US to solicit feedback concerning the number of smartphones reported lost or stolen, as well as the number of potentially duplicate IMEI or MEID identifiers that may be present. The survey results is anticipated to be completed in the fourth quarter of 2016, and the results will be shared with the TAC MDTP Working Group.

3.3 GSMA MDTP Related Activities

3.3.1 IMEI Retrieval on Disabled/Locked Devices

GSMA's Device Security Group (DSG) recognized the need to resolve the problem of extracting IMEIs from devices that have a kill switch enabled and triggered. ATIS presented its proposals to DSG, which fully endorsed and supported the mechanisms described in ATIS' "Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention", published in October 2015 (see Section 3.1.1). The specification allows the IMEI to be displayed on disabled or locked devices and DSG updated its "Anti-Theft Device Feature Requirements" to ensure alignment with the ATIS best practices.

3.3.2 GSMA Information Reporting

GSMA has developed and published a series of quarterly reports that lists the mobile carriers and countries that are connected to GSMA's IMEI Database and the degree to which IMEI data relating to devices reported lost or stolen is shared between the connected carriers. Additionally, GSMA has developed statistical reporting capabilities to provide the number of devices blocked in the USA, per carrier, per month which should help with trend analysis. The reports are designed to go some way towards addressing the lack of device theft information and they provide greater transparency on how GSMA's IMEI Database is being used to share stolen device data and what is being blocked and uploaded to the black list.

3.3.3 GSMA Carrier Recruitment

GSMA has embarked on an extensive campaign to recruit more carriers to participate in the device blocking and data sharing initiatives in the USA. Contact has been made with more than 40 licensed carriers and early efforts have secured the participation of an additional two carriers and expressions of interest from others. As part of its outreach program, GSMA is compiling feedback from those unable to commit to block devices and/or share data as to the reasons why, in order that impediments can be identified with a view to resolving them.

3.3.4 GSMA IMEI Database

GSMA continues to provide IMEI lookup services directly to device traders, law enforcement agencies and regulators and to consumers, through local database applications in a number of countries. Policy changes were introduced to ensure the widest possible access to IMEI checking

services by extending the right of access to countries not already connected to the IMEI Database. This ensures the status of devices stolen in the jurisdictions uploading data can be checked by commercial entities, authorities and consumers users in other countries thereby enhancing the value of the lookup services.

3.3.5 GSMA Device Blocking and Data Sharing Recommended Practice

GSMA has produced recommended practices to be observed by US carriers pertaining to the blocking of lost and stolen mobile devices on their networks and to the sharing of data relating to those devices via the GSMA's IMEI Database. The recommendations are designed to address inconsistencies that may exist between the individual policy, technical and process approaches adopted by the US carriers that block devices and share information via the IMEI Database. Operator alignment of approaches on a variety of aspects has the potential to resolve some perceived problems and shortcomings and is likely to result in comprehensive blocking of devices within and across all networks, timely blocking of devices within and across all networks and consistent treatment of loss and theft victims across all networks.

3.3.6 GSMA IMEI Integrity Initiatives

GSMA reviewed documentation pertaining to two of its initiatives designed to strengthen the security and integrity of IMEI implementations in devices to maintain trust and value in device blocking at a network level. Although the issue of IMEI security was de-prioritized within the FCC MDTP working group, GSMA is committed to working with device manufacturers to ensure IMEI security remains an important enabler to combat device theft.

GSMA's Device Security Group (DSG) undertook a review of the IMEI Security Technical Design Principles, which were defined to help device manufacturers develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which the IMEI mechanism is stored and the IMEI implementation itself. The review resulted in the addition of some minor changes and clarifications and, on the whole, the existing design principles were considered to be fit for purpose.

DSG also undertook a review and update of the IMEI Security Weakness Reporting and Correction process, which established a formal process to centralize the reporting of newly identified IMEI security weaknesses to the affected device manufacturers and to have those issues resolved to improve device security levels during the remaining manufacturing life cycle of the product. The original process was considered to be adequate to meet industry's needs and the only real change was a policy one that extends the right to report IMEI weaknesses, under the scheme via GSMA, to regulators and law enforcement agencies and not to restrict that right to carriers only, as had been the case.

The success of the reporting and correction process mentioned above, and achieving the overall objective of enhancing IMEI security levels, somewhat depends on IMEI security issues actually being reported. That has been a challenge for industry as carriers do not have the expertise or resources to identify IMEI security issues and/or to report them. Consequently, GSMA had previously funded and retained the services of a third party company to actively identify and report issues to be resolved. This provided industry with good visibility of the IMEI security

landscape and it ensured that identified problems were addressed. The service was discontinued in 2011 but GSMA was open to reinstating the service if there was sufficient carrier interest in it and if a business case was brought forward. DSG tried to recruit member interest to develop the required business case to define the services to be provided and to seek the necessary budget but only one carrier came forward in support. In the absence of industry interest to reinstate an IMEI security monitoring and reporting service, GSMA will focus its efforts on other activities that can have a positive impact on device theft levels.

3.3.7 GSMA Anti-Theft Device Feature Requirements

GSMA first published characteristics of kill switch features that could lead to a consistent implementation of solutions that are widely supported by operators and device manufacturers in 2014. Its document "Anti-Theft Device feature Requirements" defines a set of requirements that can be used by device manufacturers, mobile network operators, and third party service providers, to offer features to device owners to assist in locating lost/stolen devices and to protect the data within the device. The GSMA work is focused on securing the owner's device and data using software features available on the device and/or within the mobile network and the requirements have the potential to set a benchmark for anti-theft features. A further round of industry consultation and review was facilitated and a revised version of the document (version 3.0) was published that added clarity on the motivation and purpose of the work, further defined some aspects of the requirements and also added new requirements pertaining to the display of IMEIs on disabled/locked devices to align with the ATIS work on the same issue.

4 Cross Referencing Recommendations and Industry Activities

This section provides a cross reference of the FCC TAC MDTP Working Group recommendations of 2014 and 2015 with the industry MDTP related activities. This cross reference in provided in the form of two tables. Table 4.1 provides a cross reference of MDTP recommendations to industry identified in Section 2 to the associated industry MDTP activity described in Section 3. Table 4.2 provides a cross reference of the associated industry MDTP activity described in Section 3 to MDTP recommendations to industry identified in Section 2.

Editor's Note 3/17/16: The initial entries in both tables have been provided by the Editor to illustrate the proposed methodology for the completion of the cross reference information. These table entries with these initial entries are believed to be correct but should not be considered to be complete. There may be other content that may be needed to be added to these entries.

Table 4.1 Cross Reference of MDTP Recommendation to Industry MDTP Activity

Recommendation	Associated Industry Activities
Recommendation (2014) 1.4	Section 3.1.1 ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP) Section 3.3.1 GSMA IMEI Retrieval on Disabled/Locked Devices
Recommendation (2014) 1.5	Section 3.1.1 ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP) Section 3.3.1 GSMA IMEI Retrieval on Disabled/Locked Devices
Recommendation (2014) 1.6	Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2014) 1.7	Section 3.3.2 GSMA Information Reporting
Recommendation (2014) 1.15	Section 3.2.2 CTIA Stolen Phones Working Group Section 3.3.3 GSMA Carrier Recruitment
Recommendation (2014) 2.1	Section 3.3.4 GSMA IMEI Database (GSMA Liaison with CTIA)
Recommendation (2014) 2.2	Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2014) 3.1	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.2.2 CTIA Stolen Phones Working Group Section 3.2.3 CTIA Annual Survey of Consumers
Recommendation (2014) 3.2	For Reverse Logistics, industry studied the question in depth in an effort to balance the need to process mobile devices where anti-theft device credentials are not available to unlock a device (i.e. locked device with unrecoverable login credentials), and the possible threats to the security and integrity of anti-theft tools if credentials are in some way overridden. Over the course of 2014 and 2015, some industry solutions have emerged across the ecosystem to address the concern and improve reverse logistics scenarios to help consumers while maintaining the integrity of anti-theft solutions. However, it is an area that industry continues to assess challenges through ongoing work. While significant improvements have been made, it is an area that requires further study.
Recommendation (2014) 3.3	Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2014) 3.4	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.3.4 GSMA IMEI Database
Recommendation (2014) 3.5	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2014) 3.6	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2014) 3.7	This effort is underway with continuous updates being provided to the FCC by CTIA.

Recommendation	Associated Industry Activities
Recommendation (2014) 3.8	Section 3.2.4 CTIA Survey of Carriers Section 3.3.2 GSMA Information Reporting
Recommendation (2014) 3.9	Section 3.3.5 GSMA Device Blocking and Data Sharing Recommended Practice
Recommendation (2014) 4.1	
Recommendation (2014) 4.2	
Recommendation (2014) 4.3	Section 3.3.6 GSMA IMEI Integrity Initiatives Section 3.3.7 GSMA Anti-Theft Device Feature Requirements
Recommendation (2014) 4.4	7/7/16 Brian and Rob to reach to Joe Heaps on collection of data similar to the 2014 report. Section 3.2.3 CTIA Annual Survey of Consumers Section 3.2.4 CTIA Survey of Carriers
Recommendation (2015) 1.1	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.3.4 GSMA IMEI Database
Recommendation (2015) 1.2	Section 3.2.3 CTIA Annual Survey of Consumers
Recommendation (2015) 1.3	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2015) 1.4	Section 3.2.2 CTIA Stolen Phones Working Group Section 3.2.3 CTIA Annual Survey of Consumers
Recommendation (2015) 1.5	7/7/16 Brian and Rob to reach to Joe Heaps on collection of data similar to the 2014 report. Section 3.2.3 CTIA Annual Survey of Consumers Section 3.2.4 CTIA Survey of Carriers
Recommendation (2015) 1.6	7/7/16 Brian and Rob to follow-up with ATIS
Recommendation (2015) 1.7	Section 3.2.2 CTIA Stolen Phones Working Group (Voluntary Commitment)
Recommendation (2015) 1.8	Section 3.3.5 GSMA Device Blocking and Data Sharing Recommended Practice
Recommendation (2015) 1.9	Section 3.3.6 GSMA IMEI Integrity Initiatives
Recommendation (2015) 1.10	Section 3.2.4 CTIA Survey of Carriers
Recommendation (2015) 1.11	Section 3.3.6 GSMA IMEI Integrity Initiatives
Recommendation (2015) 2.1	Section 3.2.1 CTIA Mobile Device Information Portal (MDIP) Section 3.2.2 CTIA Stolen Phones Working Group
Recommendation (2015) 2.2	Section 3.2.2 CTIA Stolen Phones Working Group Section 3.3.3 GSMA Carrier Recruitment

Recommendation	Associated Industry Activities
Recommendation (2015) 2.3	As a result of the industry's Mobile Device Anti-Theft Voluntary Commitment significant anti-theft capabilities are now readily available to all consumers with enhanced feature functionality. Further, it is an area of constant innovation, advanced features and security scenarios that are based on both the physical device as well as remote access capabilities over the Internet. The ability to uniformly access the anti-theft enrolment status of a device when not in physical possession of the device requires further investigation and study in order to balance convenience, security, and privacy.
Recommendation (2015) 2.4	7/7/16 Brian and Rob to reach to Joe Heaps on collection of data similar to the 2014 report. Section 3.2.3 CTIA Annual Survey of Consumers Section 3.2.4 CTIA Survey of Carriers

Table 4.2 Cross Reference of Industry MDTP Activity to MDTP Recommendation

Industry Activity	Associated Recommendations
Section 3.1.1 ATIS Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)	Recommendation (2014) 1.4 Recommendation (2014) 1.5
Section 3.2.1 CTIA Mobile Device Information Portal (MDIP)	Recommendation (2014) 3.4 Recommendation (2015) 1.1 Recommendation (2014) 3.1 Recommendation (2014) 3.4 Recommendation (2014) 3.5 Recommendation (2014) 3.6 Recommendation (2015) 1.1 Recommendation (2015) 1.3 Recommendation (2015) 2.1

Industry Activity	Associated Recommendations
Section 3.2.2 CTIA Stolen Phones Working Group	Recommendation (2014) 1.6 Recommendation (2014) 1.15 Recommendation (2014) 2.2 Recommendation (2014) 3.1 Recommendation (2014) 3.3 Recommendation (2014) 3.5 Recommendation (2014) 3.6 Recommendation (2015) 1.3 Recommendation (2015) 1.4 Recommendation (2015) 1.7 Recommendation (2015) 2.1 Recommendation (2015) 2.2
Section 3.2.3 CTIA Annual Survey of Consumers	Recommendation (2014) 3.1 Recommendation (2014) 4.4 Recommendation (2015) 1.2 Recommendation (2015) 1.4 Recommendation (2015) 1.5 Recommendation (2015) 2.4
Section 3.2.4 CTIA Survey of Carriers	Recommendation (2014) 3.8 Recommendation (2014) 4.4 Recommendation (2015) 1.5 Recommendation (2015) 1.10 Recommendation (2015) 2.4
Section 3.3.1 GSMA IMEI Retrieval on Disabled/Locked Devices	Recommendation (2014) 1.4 Recommendation (2014) 1.5
Section 3.3.2 GSMA Information Reporting	Recommendation (2014) 1.7 Recommendation (2014) 3.8
Section 3.3.3 GSMA Carrier Recruitment	Recommendation (2014) 1.15 Recommendation (2015) 2.2
Section 3.3.4 GSMA IMEI Database	Recommendation (2014) 2.1 Recommendation (2014) 3.4 Recommendation (2015) 1.1
Section 3.3.5 GSMA Device Blocking and Data Sharing Recommended Practice	Recommendation (2014) 3.9 Recommendation (2015) 1.8

Industry Activity	Associated Recommendations
Section 3.3.6 GSMA IMEI Integrity Initiatives	Recommendation (2014) 4.3 Recommendation (2015) 1.9 Recommendation (2015) 1.11
Section 3.3.7 GSMA Anti-Theft Device Feature Requirements	Recommendation (2014) 4.3

5 Gaps in Industry MDTP Activities

Editor's Note 3/17/16: This section will identify any gaps in industry MDTP activities based upon the cross reference of the recommendations and industry MDTP activities in the two tables in Section 5.

The following table was created during the MDTP working group conference call of April 28th 2016. This table contains the four top work items identified by the member survey with bullet points of the status of these work items. This table is intended to assess in the development of the 2016 working group report.

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

- (CTIA) Nielsen survey of consumers is in the field on the effectiveness of the theft prevention. Target is summer
- (CTIA) Operator survey is currently underway to aggregate information. ETA to be confirmed.
- No action for MDTP working group until the data is available for review.
- Collection of data from LEA needs to be addressed. Will ask Joe Heaps for input on how to achieve this.

The following table was created during the MDTP working group conference call of April 28th 2016. This table contains the four top work items identified by the member survey with bullet points of the status of these work items. This table is intended to assess in the development of the 2016 working group report.
Continued studies to determine whether implementations post July 2015 have the desired effect on mobile device theft - Need to have data from CTIA and LEA from the above item before analysis can be performed. - Need the updated trend rates from LEA like those presented in the previous MDTP reports. - Additional data may be available from MDTP participants. Co-chairs to work offline with these participants to see what data may be available for this report and the working group.
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 - ATIS and GSMA best practices are in place. - May be able to evaluate implementation status of these best practices. - Education outreach should be delayed until devices are available with best practices. - FCC toolkit may be an avenue for additional input.
Consider a study on how to expand blacklisting to all US carriers, working with the GSM Association/GSMA North American Regional Interest Group and CTIA - GSMA and GSMA-NA are attempting to work with carriers in the region to encourage them to use the IMEI database. - CTIA joint meeting with GSMA discussed development of a plan to outreach to these other US carriers. Planning for 2nd joint meeting for some time in May.

6 MDTP Recommendations for 2016

Editor's Note 3/17/16: This section will contain any additional 2016 MDTP recommendations which have been identified by the FCC TAC MDTP Working Group.

7 Conclusions

Editor's Note 3/17/16: This section will contain any conclusions which have been developed by the FCC TAC MDTP Working Group.

7.1 Consumer Safeguards Survey Summary

Earlier this year, CTIA commissioned Harris Poll to conduct a survey with respect to consumer awareness and adoption of security measures. This is the third such survey since 2012. The online survey was conducted from April 14-21, 2016, using a sample from the Harris Poll Panel of 1,008 US adults who own and use a smartphone and / or tablet.

The survey found that:

- 69 percent of wireless consumers use PINs/passwords on their smartphones, up 13 percent from 2015, and up 38 percent from the first survey in 2012; and
- 51 percent have built-in remote lock and erase software installed on their smartphones, up 42 percent from 2015, and up 31 percent from 2012.
- When asked about their general security practices for their smartphones, respondents said:
- 73 percent run software updates every or almost every time on their personal smartphones;
- 51 percent of users have an anti-virus program installed on their smartphones, up 28 percent from 2015, and up 65 percent from 2012; and
- 86 percent say they are familiar with cybersecurity, defining it with protection, safety and prevention of unauthorized access.

The survey found that of the 11 percent who reported losing a smartphone, less than half – 4.7 percent – reported it was stolen, with the rest reporting it was misplaced.

Fifty-one percent of smartphone owners say they have built-in capability for remote lock / locate / erase, though only one-third of all smartphone owners have enabled the capability. One-third are not aware of such a capability being on their phone. Half of users with the capability enabled it within the last year.

Nearly half of those not enabling the lock / locate/ erase capability cite worry that they might accidentally lock or erase their data as a top reason for not enabling it. One-third cite too many passwords to keep track of, with lack of need and lack of time as other top reasons cited by 21 and 29 percent of those not enabling the capability. More information and an easier walk-through to set-up the capability are cited as encouragements to set-up by 39 and 34 percent respectively of smartphone owners who have not enabled the capability.

A follow-up focus-group with 24 respondents explored:

- Measures to address concerns users may have with access to and security of personal information (more information and notifications related to security measures);

- Sufficiency and simplicity of security features for devices and applications (most finding them fairly simple, and sufficient);
- Security settings (two-thirds configuring at time of initial set-up);
- Steps (and timing) of actions taken upon losing a mobile phone (using locator, calling phone, contracting provider, locking it remotely, wiping as a last resort); and
- Most users who have lost phones report recovering misplaced phones, with stolen phones being replaced.

7.2 Considerations for Tracking Where Stolen Mobile Phones Go

One of the questions that the MDTP Working Group has been requested to investigate is – Where do the stolen mobile phones go?

As explained below, there are many considerations and relationships which make this a difficult question to answer, particularly for cellular operators.

7.2.1 Relationship of Mobile Phones, Subscribers and Cellular Operators

In the 20th Century, there was a very close relationship between cellular operators and the mobile phones used by the subscribers. During this time, the mobile phones were heavily subsided by the cellular operators. Because of these large subsidies, the subscribers were required to purchase their mobile phones from only their cellular operator and were required to sign a service commitment with the cellular operator (a two-year service commitment was common).

However, in the 21st Century, this relationship evolved to the Bring Your Own Device (BYOD) model where the subscriber can purchase a new or used mobile phones from any seller, any store, or any reseller. The only remaining restriction is that the mobile phone must have the technical functionality required to operate on the cellular operator's network. Many of the cellular operators have web page where a subscriber can check if the make and model of their mobile phone would be compatible with the cellular operator's network.

The relationship between the user of the mobile phone and the cellular operator is via a service subscription. This service subscription is maintained in the subscriber's profile in the cellular operator network. The identification of a subscriber's profile is the Mobile Identification Number (MIN) which is the number that the subscriber provides when contacting the cellular operator's customer care and is also the number that would be dialed to call the subscriber's mobile phone. For inter-operator roaming, the International Mobile Subscriber Identity (IMSI) is used for inter-operator communications. The IMSI is the unique subscriber's MIN plus the subscriber's country identifier and the subscriber's cellular operator identifier.

The mobile phone is identified by the International Mobile Equipment Identifier (IMEI) which is generated by the mobile phone manufacturer. The IMEI contains the make and model of the mobile phone[6] as well as a unique serial number assigned by the mobile phone manufacturer.

[6] The make and model of the mobile phone is within the within the Type Allocation Code element which is the first part of the IMEI.

The IMEI only identifies the physical mobile phone, e.g., display, memory, keyboards, radios. The IMEI does not identify any associated subscribers or subscriber personalization information on the mobile phone.

On the mobile phone, the subscriber's profile is maintained in the Subscriber Identity Module (SIM). There are different versions of the SIM for 2G, 3G, and 4G networks (e.g., SIM, USIM, ISIM). The SIM may be embedded within the mobile phone or may be a removable piece of plastic and electronics as shown below:

7.2.2 Multiple Subscriptions per Mobile Phone

A mobile phone is not tied to a single subscription or a single subscriber. A mobile phone can have multiple users associated with it. One example is that the mobile phone could have two subscriptions owned by the same person – one for business calls and one for personal calls. Each subscription would have separate subscriber identities.

Subscribers with a large amount of international travel, such as between New York City and London, may want to reduce the amount of their international roaming charges. When in New York City, the subscriber could use the SIM for local New York City cellular service and when in London, the subscriber could use a second SIM for local London cellular service. The subscriber could swap the SIM cards as they travel between New York City and London. There are dual SIM mobile phones available on the market so that subscribers do not have to physically swap SIM cards as they move back and forth between different locations.

In this use case, a single mobile phone, and IMEI, is used to support two different subscriptions in two different markets and UK cellular operator is not aware that the mobile phone is being used with a US cellular operator subscription. Similarly, the US cellular operator is not aware that the mobile phone is being used with a UK cellular operator subscription.

7.2.3 Cellular Operator Visibility of Mobile Phones

The separation of the subscription from the mobile phone, which was achieved with the introduction of the SIM, means there is no need for a mobile phone to communicate or otherwise indicate its location to any network other than the one it is served by. Mobile phones do not report their movement from one cellular network to another after a SIM card is changed so the original cellular network that serves the mobile phone will never be aware if the mobile phone later connects to a different cellular network with a SIM card from the operator of that network, or a different cellular operator. Consequently, the cellular operator that previously served a mobile phone will not be aware of its migration to another cellular network and country; nor will the new cellular network be aware of the mobile phone's past history. There is no tracking of the movement of mobile phones between cellular networks with the result that cellular operators

only ever have visibility of what is currently connected to their networks and nothing beyond that.

Although cellular operators cannot track mobile phones, it is possible that OS vendors and mobile phone manufacturers may be able to do so as they continue to provide service to mobile phones that move from one cellular network and location to another but still need to be supported. OS vendors, mobile phone manufacturers and, to a lesser degree, providers of mobile app stores may be able to detect SIM changes, cellular network changes and movement from one jurisdiction to another, which could indicate, but not always definitively prove, change of mobile phone ownership. It could be possible for GSMA to provide the IMEIs of mobile phones reported lost/stolen to capable stakeholders for the purpose of tracking and reporting the movement of blacklisted mobile phone.

7.2.4 Subscription and Mobile Phone Authentication

Whenever a mobile phone is requesting service from cellular operator (e.g., at mobile phone power-on or at registration in a visited cellular network when roaming), the cellular operator must authenticate the subscriber to ensure that the subscription is authorized for service.

If the subscriber is connecting to the network of their cellular operator, the following are two of the authentication actions performed by the cellular operator:

- If the subscriber's home cellular operator performs mobile phone blacklist checking and if the mobile phone is on the blacklist, the cellular operator may deny service to the mobile phone.
- The home cellular operator will verify that the subscription is valid. If the subscription is not valid, the cellular operator will deny service to the subscriber.

If the subscriber is roaming and is requesting connection to a visited cellular operator network, the following are some of the authentication actions performed by the visited cellular operator.

- The visited cellular operator will verify that a business relationship exists between the visited cellular operator and the subscriber's home cellular operator. If there is no business relationship, the visited cellular operator will deny service to the roamer.
- The visited cellular operator will query the subscriber's home cellular operator to verify that the subscriber has a valid subscription. If subscriber does not have a valid subscription is their home cellular operator network, the visited cellular operator will deny service to the roamer.
- The visited cellular operator will query the subscriber's home cellular operator to verify that the subscriber's profile allows roaming; especially, if this an international roaming scenario. If roaming is not allowed in the subscriber's profile in their home cellular operator network, the visited cellular operator will deny service to the roamer.

There is one exception to the above authentication process. The current FCC regulations require a mobile phone without a SIM card or without a valid subscription must be able to make a call to 911 emergency services. This is referred to as an emergency call from a non-service initialized (NSI) mobile phone.

7.2.5 Mobile Phones as Wi-Fi Only Devices

The current generation of mobile phones support Wi-Fi capabilities. These capabilities help offload some of the data traffic from the cellular network and also provide connectivity when there is minimal or no cellular signal (e.g., in a basement).

The use of Wi-Fi via the mobile phone does not require the subscription and mobile phone authorization described above and no checks are carried out on whether the IMEI of the connecting mobile phone is contained in the blacklist. In fact, a mobile phone does not even need to have an installed SIM in order to use Wi-Fi connectivity and some mobile phones are used as a Wi-Fi only devices.

There are also numerous over-the-top (OTT) applications which provide messaging and voice communications on a mobile phone without the involvement of a cellular operator. These OTT applications can function via a Wi-Fi connection instead of a cellular network connection with no IMEI checks performed.

Consequently, a stolen mobile phone with could be used for web browsing, messaging, and voice communications without any involvement by any cellular operator. Since there is no cellular operator involvement, there is no opportunity to check if the mobile phone is blacklisted on the GSMA IMEI Database. However, OS vendors, mobile phone manufacturers and app store operators may have visibility of these mobile phones through the servers they operate and with which the mobile phones need to communicate to maintain service.

7.2.6 Summary

The relationships between mobile phones, subscribers, and cellular operators is summarized as follows:

- Given any valid IMSI, the associated cellular operator can be determined.
- Given any valid IMSI, the mobile number to dial to reach the mobile phone can be determined.
- Given any valid IMEI, the make and model of the mobile phone can be determined.
- Given any valid IMEI, any associated current or previous subscription associated with the mobile phone **cannot be determined**.
- Given any valid IMEI, any previous associated cellular operator, if any, **cannot be determined**.
- Any valid IMEI may be associated with multiple subscriber profiles from the same or different cellular operator networks.

- If a mobile phone has a SIM card from Operator A and the subscriber swaps that SIM card with a SIM card from Operator B, Operator A **is not aware** that the SIM card swapped has occurred and Operator A **is not aware** that the mobile phone is now associated with Operator B.

- A cellular operator **has no knowledge** about a mobile phone being used as a Wi-Fi only device or where that stolen mobile phone is being used.

Consequently, if a mobile phone is stolen from a subscriber who has service with a US cellular operator and if that stolen mobile phone is taken to a country which does not support the GSMA IMEI Database for blacklisting stolen mobile phones[7], then the US cellular operator **has no knowledge** about the mobile phone stolen from their subscriber being placed in service in that other country.

Additionally, there are **no mechanisms** for the US cellular operator to find where a specific mobile phone is being used in any other cellular operator around the world. This is especially true for stolen mobile phones that are used only in the countries that does not support the blacklist of the GSMA IMEI Database[8].

Finally, if the stolen mobile phone is used as a Wi-Fi device with OTT applications for web browsing, messaging, and voice communications, the entire global cellular network is completely unaware of the operation of this stolen mobile phone. Thus, a US cellular operator would have no knowledge if the stolen mobile phone is being used as a Wi-Fi device and if that is the case then the US cellular operator would have no knowledge where the stolen mobile phone is being used. However, other ecosystem players such as OS vendors, mobile phone manufacturers and operators of app stores may be able to identify and flag changes of ownership and location of mobile phones that are known to have been reported lost/stolen and blacklisted on GSMA's IMEI Database.

[7] Another variant is that the cellular operator in the other country is connected to the GSMA IMEI Database but does not take the blacklist data that the US cellular operator has posted on the GSMA IMEI Database.
[8] Ibid.

Appendix A: Glossary

FCC	**Federal Communications Commission**
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**
MDIP	**Mobile Device Information Portal**
MDTP	**Mobile Device Theft Prevention**
MEID	**Mobile Equipment Identifier** A MEID is a globally unique number identifying a physical piece of CDMA2000 mobile station equipment. The number format is defined by the 3GPP2 report S.R0048.
MIN	**Mobile Identification Number** The MIN, more commonly known as a 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**
RFP	**Request for Proposal**

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.)
SPWG	**Stolen Phones Working Group**

Appendix B: MDTP Parking Lot

This appendix contains the parking lot items which have been identified by the FCC TAC MDTP Working Group.

Automated Process for Returning Stolen Property to Rightful Owner (Added 4/28/16)

In effect, when LE comes into possession of a smartphone that is either blacklisted, bricked, locked, or otherwise, there is effectively nothing to be done on the LE end. The device goes into a storage locker, and that's the end of it. This is bad for consumers and bad for law enforcement, too.

Generally, the blacklisted, bricked, locked or similar scenario suggests that the phone is either lost or stolen - and as a result there will seldom be probable cause to issue a subpoena to review the contents of the device. In the event that it is in the possession of a suspect at the time that LE comes into contact with the device there MIGHT be PC to issue a subpoena, but this is unlikely, and absent such a showing it is generally impossible to determine whether the individual in possession of the phone stole it, or if they are in receipt of stolen property.

To solve this issue, here is a suggested automated process that could be setup that would aid consumers and law enforcement:

1. When LE comes into contact with a device that is blacklisted, blocked, bricked, etc., they run the readily identifiable IMEI number in an FCC (or CTIA?) maintained database, and the LE agency inputs their contact information into the database as part of the automated report that they file.
2. This is a one-way communication - which notifies the last known carrier associated with that IMEI # that X,Y, or Z law enforcement agency has custody of one of their consumer's smartphones.
3. The carrier NOTIFIES the consumer (via mail, e-mail, etc.) that their device has been found, and provides the LE agency's contact information.
4. The consumer has the option to contact the Law Enforcement agency that is in-custody of their device and can retrieve THEIR property.

When law enforcement recovers a device but cannot determine who the rightful owner is there is no way to prosecute, and accordingly there is no accountability. As a result there is less deterrent to engage in the behavior, and repeat offenders are more likely to attempt to steal devices until they get one that is not bricked. Prosecutors have to be able to prove that the individual in possession of the device was not authorized to be in possession of the device. This is impossible if the owner of the property does not come forward to identify that it is their smartphone, and that the individual who had their device was not supposed to have it.

Is there a reason such a solution has not been given consideration? Is there something I do not understand that precludes such a solution to this problem?

Revision History

Date	Version	Description	Author
3/18/16	0.01	Initial report skeleton constructed by the Editor based upon instructions provided during the March 17th 2016 MDTP working group call.	DeWayne Sennett (Editor)
4/28/16	0.02	Incorporated the real-time modifications to Section 5 which were applied during the April 28th 2016 MDTP working group call. Incorporated the following Editor's assignments and actions: - Added new Appendix B for MDTP Parking Lot items - Updated membership with updates received via email.	DeWayne Sennett (Editor)
6/2/16	0.03	Incorporated the following changes that were applied during the June 2nd MDTP conf call: - Added a level 3 heading for Section 3.2.2 CTIA Stolen Phones Working Group - Added an Editor's Note to Section 3.3 indicating that this section needs to capture all of the GSMA MDTP activities Also removed Jeff Brannigan of the Department of Homeland Security (DHS) from the membership list per his request.	DeWayne Sennett (Editor)
7/7/16	0.04	Incorporated the notes of actions and assignments to entries in Table 4-1 which were identified during the July 7th MDTP conf call. Also changed the Asurion representative in the membership list from Mark Romer to Ogechi Anaytonwu.	DeWayne Sennett (Editor)
7/22/16	0.05	Incorporated the contribution from John Marinho with the descriptions of the CTIA activities for Section 3 and the mapping of the CTIA activities to recommendations in Table 4.1 which was accepted during the July 21st 2016 FCC TAC MDTP conference call. Incorporated the following Editor's Actions: -Updated Table 4.2 based upon the updates to Table 4.1. - Editor's Note in Section 3.2 "CTIA MDTP Related Activities" has been deleted. - Acronym list has been updated. - Added Jack Mcartney of Recipero to membership list.	DeWayne Sennett (Editor)
8/4/16	0.06	Incorporated the contribution from James Moran of GSMA which provides the description of GSMA activities for section 3.3 as well as the mappings for Table 4.1 and 4.2. This contribution was accepted during the August 4th 2016 FCC MDTP Working Group call.	DeWayne Sennett (Editor)
9/1/16	0.07	Incorporated the real time updates from the Sept 1st 2016 MDTP working group call.	DeWayne Sennett (Editor)
10/4/16	0.08	Incorporated the CTIA Consumer Safeguards Survey Summary as new subsection 7.1 in Section 7 Conclusions.	DeWayne Sennett (Editor)

Date	Version	Description	Author
11/13/16	0.09	Incorporated the following contributions which were accepted during the November 10th 2016 MDTP conference call: - John Marinho's contribution to Table 4.2 for Recommendation (2014) 3.2 and Recommendation (2015) 2.3. - Contribution for Conclusions Section on tracking where stolen mobile devices go.	DeWayne Sennett (Editor)