Technological Advisory Council (TAC) Mobile Device Theft Prevention (MDTP) Working Group

Version 1.0

December 5, 2018

Table of Contents

Executive Summary

This report provides an overview of the Mobile Device Theft Prevention Working Group's (MDTP WG) efforts to reduce mobile device theft throughout its history and specifically in response to the requests made of the group for the 2018 calendar year by the FCC's Chairman.

Since its inception, the MDTP WG has made significant strides towards creating solutions to help deter the criminal theft of mobile devices. These solutions include coordinating a voluntary industry-led effort to implement recommendations for consumer anti-theft features and the development of the Stolen Phone Checker—a tool, powered by the GSMA Device Check service—that enables consumers, commercial entities, and law enforcement to verify whether a device has been reported lost or stolen.

Anecdotal evidence suggests that these and other efforts are having an impact. The Stolen Phone Checker, which was released in May 2017, has already resulted in more than a million queries. And consumer survey results show that consumers are increasingly adopting security features on their mobile devices. In fact, an analysis of these survey results indicates that between 2016 and 2018, the number of consumers impacted by mobile device theft has dropped dramatically. Our estimate suggests that theft of mobile devices has declined by more than 50 percent.

During the 2018 session, the MDTP WG worked to:

- Identify sources of statistics that could be used to study future mobile device threats and trafficking across international borders, as well as make further recommendations to mitigate device theft;
- Continue partnering with law enforcement to assess the benefits of the information portal (*i.e.* stolenphonechecker.org) to relevant stakeholders and identify potential enhancements;
- Develop baseline statistics on device theft based on data from directed consumer surveys and law enforcement to help track long-term progress and identify theft scenarios.

While the group has seen overall success, challenges remain with regard to these areas. The MDTP WG puts forth ten actionable recommendations for consideration that it believes will help to solve some of these challenges and move towards continued success in the fight to combat criminal mobile device theft.

1 History of MDTP WG and Achievements

1.1 *Efforts of MDTP WG*

The Federal Communications Commission (“FCC) Technological Advisory Council’s (“TAC”) Mobile Device Theft Prevention (“MDTP”) Working Group (“WG”) has been collaborating for more than four years on solutions to the challenge of criminal theft of mobile devices, principally smartphones. The problem was identified by local law enforcement as a key challenge, and solutions were sought by industry, consumer protection advocates, and law enforcement. At one point, law enforcement found that in major American cities, such as Washington, D.C., and New York, roughly 40 percent of all robberies involved smartphones.

The MDTP WG is made up of representatives from carriers, manufacturers, smartphone recyclers, third-party solution providers, industry associations, and federal, state and local law enforcement. The WG made a wide range of recommendations in 2014 and in 2015 that focused on technical solutions to device theft, consumer education, and information sharing. Technical solutions included dedicated work by the Alliance for Telecommunications Industry Solutions (“ATIS”) to develop policies, methods, or procedures for law enforcement to obtain device identifiers from smartphones in their possession. The WG also recommended steps to explore blacklists and methods for consumers to be able to look up a smartphone’s International Mobile Equipment Identifier (“IMEI”)/Mobile Equipment Identifier (“MEID”) status, and a mechanism for consumers to check the enrollment status of a device. Other recommendations included educating consumers about how they can protect their data and their smartphones to augment efforts undertaken by the FCC and law enforcement.

1.2 *Industry Voluntary Commitment to Include Anti-Theft Tools on Devices*

A key part of the initial work of the MDTP WG was to develop recommendations for visible opt-out anti-theft features to be embedded within mobile devices for consumer use. MDTP WG members responded by coordinating a vigorous and dynamic voluntary industry-led effort among mobile device manufacturers to implement these recommendations. In an April 10, 2012 voluntary commitment, industry participants took steps to deter theft, and in the Smartphone Anti-Theft Voluntary Commitment of 2014, industry participants agreed to provide remote capabilities to wipe information from new smartphones, among other security measures.

The Smartphone Anti-Theft Voluntary Commitment provides that:

New models of smartphones first manufactured after July 2015 for retail sale in the United States will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones and provides the connected capability to:

1. Remotely wipe the authorized user’s data (i.e., erase personal info that is added after purchase such as contacts, photos, emails, etc.) from their smartphone in the event it is lost or stolen.

2. Render the smartphone inoperable to an unauthorized user (e.g., locking the smartphone so it cannot be used without a password or PIN), except in accordance with FCC rules for 9-1-1 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., “phone home”).

3. Prevent reactivation without the authorized user’s permission (including unauthorized factory reset attempts) to the extent technologically feasible (e.g., locking the smartphone as in 2 above).

4. Reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible (e.g., restored from the cloud).

Each network operator signatory commits to permit the availability and full usability of a baseline anti-theft tool that can be preloaded or downloaded on a smartphone as specified in this commitment.

1.3 Stolen Phone Checker

Based on the efforts and recommendations of the TAC MDTP WG, CTIA—The Wireless Association (“CTIA”) launched the Stolen Phone Checker in May 2017. The Stolen Phone Checker—powered by the GSMA Device Check service—is a public service designed to limit the resale of lost and stolen mobile devices in the United State and to help consumers, businesses, and law enforcement agencies learn the status of a device and ultimately make informed choices. When launched, this service garnered significant national media coverage, and this coverage continues today.

1.4 Impact of Increased Public Awareness of Tools Available to Mitigate Mobile Device Theft

1.4.1 Industry Efforts to Raise Public Awareness

Over the last several years, both industry and government have worked hard to combat the problem of mobile device theft and to inform consumers of ways to protect themselves. Industry makes available numerous resources for consumers to protect their devices and their data, including tools to deter and prevent theft, help consumers recover a lost or stolen device, and remotely manage data in the instance that their device cannot be found. Industry has taken steps to make it easy for users to enable these features. For example, on iOS, when a user signs into iCloud as part of setting up a new device, Find My iPhone is enabled automatically and links the device to their account. This functionality helps end-users locate and protect their devices by viewing device location on a map, playing sounds to help find the device, and remotely locking and or erasing personal information from a missing device. Most major carriers who provide the ability to "bring your own phone" to their networks also offer web-based tools for consumers to look up IMEI numbers. Aimed at addressing mobile theft, these services are almost always accompanied by explicit policies to not activate devices that have been reported lost or stolen.[1]

Beyond CTIA's Stolen Phone Checker, CTIA has also developed a variety of new consumer-centric cybersecurity resources over the past year, including a just-released series of "how to" videos on important cybersecurity topics, such as how to set up a device passcode, how to engage "find my phone" anti-theft tools, and what to do if your device is lost or stolen. Industry also continues to educate consumers about how they can protect their devices and personal data. CTIA regularly updates its consumer resource pages to ensure consumers have access to the latest recommendations on how to protect against cyber threats and device theft.[2]

GSMA's IMEI Database[3] allows operators to exchange data and to block devices that are "blacklisted," *i.e.*, reported lost or stolen using a device's IMEI.[4] Device Check service allows entities to query the GSMA IMEI database to provide up to 10 years of a device's history as well as the device model information and capabilities. It serves to help resellers identify and eliminate stolen devices before they can enter supply chains, confirm the true device model for authenticity and calculate device value, discourage device theft by reducing the value of a stolen device, and confirm the network operator that reported a device stolen or lost, which helps with repatriation to the rightful owner.[5]

[1] *See, e.g.*, AT&T, *Bring your own device to AT&*T (last visited Oct. 9, 2018), https://m.att.com/shopmobile/wireless/byop/checkIMEI.html; Sprint, *Bring your own device*, (last visited Oct. 9, 2018), https://www.sprint.com/en/shop/bring-your-phone-to-sprint.html; T-Mobile, *IMEI Status Check*, (last visited Oct. 9, 2018), https://www.t-mobile.com/verifyIMEI.aspx; U.S. Cellular, *Is you Smartphone or Tablet Compatible*, (last visited Oct. 9, 2018), https://www.uscellular.com/bring-your-own-device/index.html; and Verizon, *Let's get started by checking your old device*, (last visited Oct. 9, 2018), https://www.verizonwireless.com/prospect/bring-your-own-device/#/checkDevice.

[2] *See* CTIA, Consumer Resources, https://www.ctia.org/consumer-resources/preventing-device-theft; https://www.ctia.org/consumer-resources/protecting-your-data.

[3] *See* GSMA, IMEI Database (last visited Oct. 9, 2018), https://www.gsma.com/services/tac-allocation/the-imei-database/.

[4] *See* GSMA, IMEI Blacklisting (last visited Oct. 9, 2018), https://www.gsma.com/services/gsma-imei/device-theft/.

[5] *See* GSMA, GSMA Device Check (last visited October 9, 2018), https://www.gsma.com/services/gsma-imei/about-device-check/.

GSMA also provides additional services aimed at reducing the number of lost or stolen devices, including consumer tips on mobile phone theft.[6] GSMA has also recently developed a pilot program—the Third Party Blacklisting Pilot Program—that allows certain operator-approved entities to directly contribute to the GSMA Black List.

1.4.2 Federal Government Efforts to Raise Public Awareness

The Federal Government has expanded the resources it provides to the public and has promoted awareness and common-sense solutions, including better use of the tools already available to deter theft and safeguard data. For example, the Federal Communications Commission ("FCC" or "Commission") lists tips to safeguard against smart device theft and protect data on a phone[7] and the Federal Trade Commission provides guidance on locking, updating, finding, and reporting a phone missing.[8] The FCC also lists numbers of cellular service providers for victims to report stolen smart devices.[9] Additionally, we have seen action taken by the United States Department of Justice to prosecute those who traffic in stolen devices.[10]

1.4.3 Law Enforcement Efforts To Raise Public Awareness

Law enforcement can play an important role in highlighting anti-theft features. Numerous law enforcement authorities are engaged in public awareness and education campaigns to stem mobile phone theft and share industry and federal resources with their residents. The Washington, D.C. Metropolitan Police Department, for example, launched a public campaign urging victims of mobile phone theft to "brick it." If a device is stolen, the owner should contact the carrier and have the device remotely disabled because, "[i]f a smart phone is rendered inactive in such a manner, it's often considered to be as useful as a 'brick.' These 'bricked'

[6] *See* GSMA, Mobile Phone Theft (last visited Oct. 9, 2018), https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-advice-for-mobile-phone-users/mobile-phone-theft.

[7] *See* FCC, Protect Your Smart Device (last visited Oct. 9, 2018), https://www.fcc.gov/consumers/guides/protect-your-mobile-device.

[8] FTC, Sheryl Roth, An identify thief stole my phone! (June 8, 2017), https://www.consumer.ftc.gov/blog/2017/06/identity-thief-stole-my-phone.

[9] FCC, How to Report a Lost or Stolen Smart Device (last visited Oct. 9, 2018), https://www.fcc.gov/consumers/guides/how-report-lost-or-stolen-smart-device.

[10] *See e.g.* US DOJ, *Golden Valley Man Convicted of Leading Multi-Million Dollar Cell Phone Trafficking Conspiracy* (June 15, 2016), (https://www.justice.gov/usao-mn/pr/golden-valley-man-convicted-leading-multi-million-dollar-cell-phone-trafficking) (announcing conviction of man who led a conspiracy to traffic more than $3.8 million in stolen cellular devices throughout the United States and Hong Kong); U.S. DOJ, *Operator of D.C. Electronics Store Found Guilty of Trafficking In Stolen Property and Related Charges – Stolen iPhone Was Recovered From His Business* (Jan. 17, 2014), (https://www.justice.gov/usao-dc/pr/operator-dc-electronics-store-found-guilty-trafficking-stolen-property-and-related) (announcing conviction of operator of electronics store after victim of phone theft used "Fine My iPhone" to tracked the stolen device to the store).

phones are of little use to thieves because they can't be reactivated after being sold on the black market."[11]

Similarly, the City of San Francisco established an "eyes up, phones down" anti-crime and public awareness campaign, providing tips to outsmart thieves and protect individuals' devices. New York Police Department (NYPD) has also established campaigns to raise awareness of available tools, including a robust campaign to actively encourage residents to upgrade to iOS 7 to activate available anti-theft tools.[12] Campaigns such as these can help to raise both consumer awareness and adoption of anti-theft tools and best practices.

1.4.4 Other Resources

Other resources abound as well, including checklists and tips to protect consumers produced by a range of security- and consumer-focused organizations. Consumer Reports outlines that users should adopt practices such as using strong passwords for lock screens, enabling a "find my phone" application, and backing up a phone's information.[13] Other organizations, like Norton, encourage users to immediately report the loss of a cell phone to the carrier, remotely lock and wipe the phone, and change sensitive passwords which might be saved on the device.[14]

1.4.5 Impact on Mobile Device Theft

The MDTP WG has reviewed the effectiveness of these and other efforts to raise awareness and increase the use of tools to protect against and recover from mobile device theft. Consumer education appears to have had a substantial impact on the practices of consumers and has helped to ameliorate this public safety and consumer protection challenge.

A recent Harris Poll, commissioned by CTIA to survey consumer awareness and adoption of cybersecurity features and tools, shows that America's wireless consumers continue to adopt anti-theft features and more advanced security measures for their mobile devices amid ongoing consumer protection and education efforts. Nearly 60 percent of American smartphone owners

[11] *See* Metropolitan Police Department, Stolen Smart Phone? Brick It! (last visited Oct. 9, 2018), https://mpdc.dc.gov/page/stolen-smart-phone-brick-it.

[12] *See* NYPD, *NYPD Operation ID*, ID.http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/iPhone3.pdf; New York Post, *NYPD urges Apple iOS7 download* (Sept. 24, 2013), https://nypost.com/2013/09/24/nypd-urges-apple-ios7-download/; Apple Insider, *US prosecutors encourage users to upgrade to iOS7 for Activation Lock security feature* (Sept. 19, 2013), https://appleinsider.com/articles/13/09/19/us-prosecutors-encourage-users-to-upgrade-to-ios-7-for-activation-lock-security-feature.

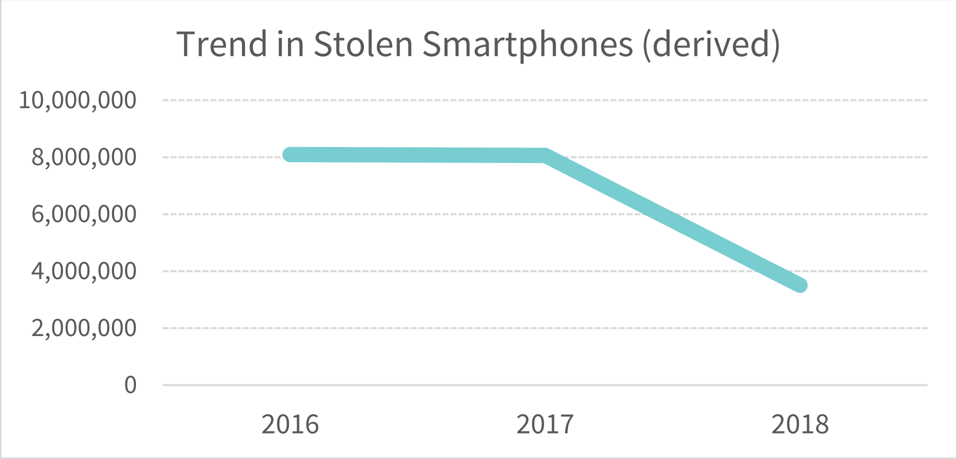
[13] *See, e.g.*, Consumer Reports, *5 steps to protect your smart phone from theft or loss* (Apr. 2014), https://www.consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm.

[14] *See, e.g.*, Norton, *3 Steps to Take Immediately if Your Phone is Stolen or Lost*, https://us.norton.com/internetsecurity-mobile-what-to-do-if-your-smartphone-is-lost-or-stolen.html.

reported being aware that they have the "find your phone" capability on their device, allowing them to remotely locate, lock, and erase their smartphones.

The MDTP WG attempted to determine the effect of these efforts on the number of consumers impacted by mobile device theft. Using the Harris Poll survey results and publicly available data on the U.S. population, the WG was able to derive that between 2016 and 2018 the number of consumers impacted by mobile device theft has dropped dramatically. Our estimate suggests that theft of mobile devices has declined by more than 50 percent and is consistent with anecdotal press reports from key U.S. cities. The timing appears to align with introduction of the anti-theft tools and Stolen Phone Checker, but further study is required to determine whether there is a correlation.

Chart 1.1: Trend in Stolen Smartphones



2 2018 Tasking of Federal Communications Commission Chairman

For 2018, the WG was asked to build on earlier work and attempt to identify statistics that help support anecdotal evidence suggesting a steep decline in device theft and also focus on international engagement to determine where stolen devices ultimately end up. Specifically, the Chairman tasked the MDTP WG with the following:

- Focus on supporting FCC efforts in working with foreign regulatory agencies to combat the theft and use of illegal mobile devices, including working to identify where devices go once they are stolen.
- Reassess the effectiveness of the information portal and make recommendations, as appropriate, for its future improvement.

- Study whether mobile device theft has declined in the United States since these efforts have been implemented.

With this tasking, the MDTP WG focused on three primary areas:

- Study future mobile device threats and trafficking across international borders and make further recommendations.
- Continue to work with law enforcement to assess the benefits of the information portal (*i.e.* stolenphonechecker.org) to relevant stakeholders and identify potential enhancements.
- Develop baseline statistics on device theft based on data from directed consumer surveys and law enforcement to help track long-term progress and identify theft scenarios.

2.1 MDTP WG Membership

Table 1.1: MDTP WG Membership

Name	**Organization**
Melanie K. Tiano, Chair	CTIA
Jason Novak	Apple
Maria Kirby	Apple
Brian K. Daly	AT&T
John Marinho	CTIA
Joseph Heaps	Department of Justice (DOJ), National Institute of Justice
Max Santiago	ecoATM
Kevin Harris	ecoATM
James Moran	GSM Association
Thomas Fitzgerald	New York City Police Department
Joseph Hansen	Motorola Mobility
Joel Voss	Motorola Mobility
Jack McArtney	Recipero
David Dillard	Recipero
Les Gray	Recipero
Mark Harmon	Recipero
Dennis Roberson (TAC Chair)	Roberson and Associates
Bill Alberth	Roberson and Associates
Robert Kubik	Samsung
Maxwell Szabo	City and County of San Francisco
Steve Sharkey	T-Mobile USA
Gary Jones	T-Mobile USA
Mark Younge	T-Mobile USA

Name	Organization
Samuel Messinger	United States Secret Service

3 Stolen Phone Checker

CTIA's Stolen Phone Checker lets consumers, law enforcement, and commercial users know if a mobile device has been reported lost or stolen. This information is beneficial for consumers and commercial entities—including third-party resellers of mobile devices—to alert them to the status of a device before they make a purchase or a sale. If a device is "reported lost or stolen" it means that an owner reported the device is no longer in his/her possession; the wireless carrier confirmed the device was stolen due to fraud; and/or the wireless carrier confirmed the owner is not in possession of the device.

By inputting a device's unique serial number or International Mobile Equipment Identifier (IMEI) into the database, users of the Stolen Phone Checker have instant access to the world's largest collection of data concerning reported lost or stolen phones provided by carriers, including information on different device models and their capabilities. If the device has been blocked, it will be marked with a red warning status and will highlight that it might not be able to access mobile networks. GSMA Device Check, which powers the service, contains regularly refreshed data supplied by over a hundred carriers internationally, including U.S. operators AT&T, Sprint, T-Mobile, U.S. Cellular and Verizon Wireless.[15]

The tool allows consumers, commercial entities, and law enforcement representatives to check devices based on IMEI, mobile equipment identifier (MEID), or electronic serial number (ESN) identifiers.

For consumers, the tool provides simple instructions and guidance, including tips on how users can better protect themselves by utilizing PINs, passwords, apps, and other security features—such as using apps to locate, lock, and/or erase a wireless device if it is lost or stolen[16]—and instructions on how to contact their wireless carrier and local law enforcement.[17]

The Stolen Phone Checker also helps protect commercial users and businesses such as device resellers or retailers, insurers, repair centers, recyclers, and other companies in the wireless

[15] *See* GSMA, *GSMA Device Check Powers CTIA's Stolen Phone Checker* (May 18, 2017), https://www.gsma.com/newsroom/blog/gsma-device-check-powers-ctia-stolen-device-checker-service/.

[16] *See* CTIA, Stolen Phone Checker, FAQ (last visited Oct. 9, 2018), https://stolenphonechecker.org/spc/faqs.jsp

[17] *See* CTIA, Stolen Phone Checker, Consumer (last visited Oct. 9, 2018), https://stolenphonechecker.org/spc/consumer.

ecosystem and includes use case examples.[18] It also helps law enforcement agencies discourage device theft, identify and check the lost or stolen status of a recovered device, and identify the wireless carrier associated with a device reported to the GSMA Black List.[19]

3.1 Usage

As explained above, the Stolen Phone Checker is available to consumers, law enforcement, and commercial users, including retailers, resellers, and recyclers of devices, along with insurers, repair centers, and providers of solutions to help identify or prevent the use of lost or stolen devices. Since its launch in May 2017, more than one million queries have been made using the database.[20] Commercial users make up the majority of users, followed by consumers, and then law enforcement. As will be discussed below, the WG and industry has continued to make efforts to increase awareness of this tool to both consumers and law enforcement.

3.2 Evolution

The Stolen Phone Checker tool was created to assist with combatting mobile device theft. The MDTP WG has explored what improvements can be made to the database to make it an even more useful tool for consumers, commercial users, and law enforcement. Two possibilities have arisen: (1) develop the ability to use the Stolen Phone Checker as a tool to help mitigate the problem of contraband phones in prisons; and (2) find ways to streamline the onboarding process, making it easier for individual law enforcement officers to take advantage of the tool.

3.2.1 Contraband Reason Code

In February 2018, the FCC, under the leadership of Chairman Pai, convened a stakeholder meeting to discuss solutions to contraband cell phones in state correctional facilities. Chairman Pai explained the initiative's goal as follows: "to bring together a diverse group to determine the most effective, affordable, and safe ways to address this problem—that is, to stop the threat of contraband cell phones without causing harm to legitimate wireless users."[21] During the February stakeholder meeting, CTIA, on behalf of the wireless industry, proposed the creation of

[18] *See* CTIA, Stolen Phone Checker, Commercial (last visited Oct. 9, 2018), https://stolenphonechecker.org/spc/commercial.

[19] *See* CTIA, Stolen Phone Checker, Law Enforcement (last visited Oct. 9, 2018), https://stolenphonechecker.org/spc/law.

[20] *See* CTIA, *CTIA Stolen Phone Checker Service Hits Major Milestone in U.S. Wireless Industry Efforts to Combat Smartphone Theft* (Nov. 1, 2018) https://www.ctia.org/news/ctia-stolen-phone-checker-service-hits-major-milestone-in-u-s-wireless-industry-efforts-to-combat-smartphone-theft

[21] Press Release, *Chairman Pai Convenes Meeting to Discuss Combatting Contraband Wireless Devices in Correctional Facilities* (Feb. 7, 2018), https://docs.fcc.gov/public/attachments/DOC-349082A1.pdf.

a task force to serve as a forum for further dialogue, as an organizing body for testing technologies, and as a means to combat contraband devices generally.

In April, the Contraband Phone Task Force held its first meeting in Washington, D.C. The task force consists of wireless industry representatives, state correctional department officials, the Department of Justice's Bureau of Prisons, and the FCC. The task force has since held several additional face-to-face meetings and plans to hold its next meeting in January at the Association of State Correctional Administrators' (ASCA) annual winter conference in New Orleans.

The task force has explored a variety of potential solutions to address this challenge, including identifying and testing ways to stamp out the use of contraband cell phones, generally known as Contraband Interdiction System (CIS) technologies.[22] The task force has also been developing a court order process to direct wireless providers to disable service to devices identified as contraband. In addition, the task force is working to modify the GSMA Black List for use in combatting contraband devices, specifically by adding a Reason Code dedicated to contraband phones. Over the past six months, the wireless industry has worked closely with several states to develop a court order process and has effectively disabled service to hundreds of contraband phones. Adding the Contraband Reason Code to the Stolen Phone Checker, via the GSMA Black List, will further assist corrections officials in combatting contraband devices.

3.2.2 Efforts to Streamline the Onboarding Process for Law Enforcement

As described in greater detail below, there are approximately 18,000 different law enforcement agencies throughout the United States at the federal, state, and local levels. Each of these agencies has their own processes for approving contracts and managing their own investigative procedures. Several agencies have reported challenges with the process necessary to be onboarded to use the Stolen Phone Checker. Possible solutions are being explored.

3.3 Efforts to Increase Awareness and Use of Stolen Phone Checker

Since the inception of the Stolen Phone Checker last year, the industry has worked to increase awareness. In particular, CTIA has worked to share information related to the Stolen Phone Checker, including capabilities and how to sign up, through op-eds and written collateral circulated among law enforcement agencies.

In addition to these efforts, the law enforcement community is also working to help raise awareness. In November, the International Association of Chiefs of Police (IACP) adopted a

[22] Press Release, CTIA and ASCA Statement on Contraband Phones Task Force Meeting (Apr. 30, 2018), https://www.ctia.org/news/ctia-and-asca-statement-on-contraband-phones-task-force-meeting.

resolution to further encourage mobile network operators worldwide to participate in the global GSMA IMEI Blacklist database.[23]

3.4 Recommendations

Since its launch in May 2017, the Stolen Phone Checker has been increasingly adopted by consumers, commercial resellers, and law enforcement—more than one million queries have been made. While this is a successful and promising start, the MDTP WG recommends that:

a. CTIA and GSMA monitor the Stolen Phone Checker to identify possible enhancements and make any necessary changes to increase effectiveness and encourage broader adoption, including efforts to streamline law enforcement access to and enrollment in the Stolen Phone Checker service.
b. The FCC continues to promote the Stolen Phone Checker to consumers, retailers and traders of devices, and throughout the law enforcement community, possibly through engagement with local law enforcement agencies and with law enforcement associations, such as the IACP.

4 Law Enforcement Coordination and Statistics

4.1 Overview of US Law Enforcement Agencies

In the United States, multiple law enforcement entities have a stake in combatting mobile device theft. Local police departments and transit authorities are on the front lines of robbery and theft investigations and prosecutions. Federal entities have a stake in understanding, preventing, and investigating interstate and international criminal activity, including identity theft and the global trade of stolen phones, which can be used in other criminal enterprises. There are approximately 18,000 law enforcement agencies in the United States, in diverse jurisdictions and at varied levels. As a result, there is no single law enforcement entity that can address all aspects of the problem of stolen mobile devices, from the initial theft to the global ecosystem of stolen phones. In addition, there is no uniform mechanism across these agencies to track the number of mobile devices stolen or report them in any manner that can be reliably aggregated.

The breadth and diversity of the stakeholders involved is partially reflected in the MDTP WG's membership, which draws from the City and County of San Francisco, the New York City Police Department and the United States Secret Service. Attempts by the MDTP to develop enduring relationships for tracking of mobile device thefts as well as outreach have been hampered by the

[23] *See* International Association of Chiefs of Police, *Combatting the Global Black Market for Stolen Mobile Devices* (Nov. 2018), https://www.theiacp.org/resolutions.

number of organizations represented and the fluidity of personnel. It has been noted that collection of crime statistics at a national level is driven by specific definitions of the crimes to be tracked and that covering a large portion of law enforcement agencies in the reporting process would require changes in the federal reporting process. This is outside the scope of TAC. Viable efforts in this area under MDTP recommendations will focus on industry efforts to consolidate data from currently available sources as well as work with identified law enforcement agencies who have determined tracking mobile device theft to be within their domain of responsibility.

4.2 Mobile Device Theft Statistics

4.2.1 Challenges with Acquiring Voluntary Statistics from Law Enforcement

As the FCC knows, there are challenges to collecting meaningful, comparable law enforcement data. Data about the motive for theft, the property stolen in a robbery, or the use of anti-theft tools by victims are hard to obtain because they are not routinely collected by law enforcement around the country. More generally, law enforcement agencies often have different obligations when it comes to collecting data under varied local, federal, and state laws.

Those that do collect data may collect and categorize their data differently and for different purposes. The Bureau of Justice Statistics in the United States Department of Justice aptly summarizes some of the many complexities in data gathering and analysis from varied states and localities. "Many persons … at the local, state, and federal levels work to ensure the quality of this information [in uniform crime statistics]. However, given the magnitude of the work, there may be inaccuracies in some of the reported data. BJS is responsible for accurately transcribing the FBI data, but not for the quality of the underlying information."[24]

State and local law enforcement agencies do not routinely collect the sort of information that would be most helpful to track mobile device theft comprehensively, and local governments are often addressing more pressing matters than answering calls for data. Observers have noted in the context of standardizing information sharing that "state and local governments are traditionally skeptical when it comes to the federal imposition of standards."[25] And in other research areas, it has been noted that "it's not possible to analyze and compare data from all the

[24] BJS, Arrest Data Analysis Tool, https://www.bjs.gov/index.cfm?ty=datool&surl=/arrests/index.cfm "[A]rrest reports by age, sex, and race provide valuable data on 43 offenses including violent, drug, gambling, and larceny crimes." Uniform Crime Reporting Program Data: Arrests by Age, Sex, and Race, United States, 2016 (ICPSR 37056) at https://www.icpsr.umich.edu/icpsrweb/NACJD/studies/37056

[25] DigitalCommunities.com, Law Enforcement Information Sharing and the Implications for Local Government (A Technical Reference) https://cdn.ymaws.com/www.ijis.org/resource/collection/232074EF-6453-4014-BC4E-018BF818D291/Law_Enforcement_Information_Sharing_and_the_Implications_for_Local_Government.pdf

agencies because each department collects information differently…. The size of an agency and the size of its jurisdiction, as well as overall crime rates, also need to be taken account."[26]

4.2.2 Summary of Statistics Available to the MDTP WG

The MDTP WG was tasked with obtaining statistics and data to examine the impact of efforts to combat mobile device theft. While the MDTP WG continued to face challenges acquiring statistics and data from law enforcement directly, data from survey results and publicly available sources continues to indicate an increase in consumer awareness and a decline in mobile device theft overall.

4.2.2.1 CTIA's Commissioned Harris Poll Survey

One of the goals of the MDTP WG was to analyze statistics to determine the impact of the available tools and resources on mobile device theft. CTIA annually commissions Harris Poll to conduct surveys with respect to consumer awareness and adoption of security measures, including the adoption of anti-theft security tools on smartphones.

This is the fifth such survey conducted since 2012. An online survey was conducted in May 2018, using a sample from the Harris Poll Panel of 1,007 U.S. adults who own and use a personal smartphone, tablet, or both. The survey population was representative of the demographics of the United States population. In-depth interviews of select survey respondents were conducted the week of August 6, 2018.

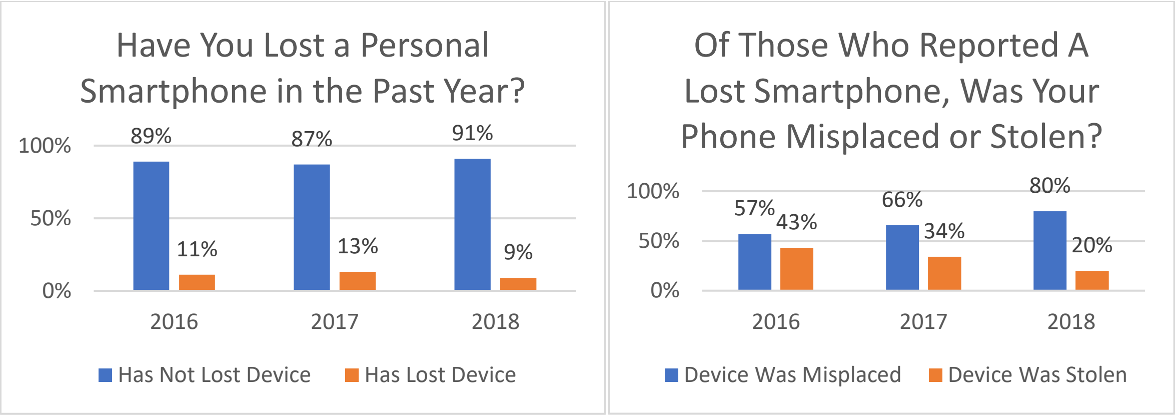
The survey confirmed that consumers continue to adopt strong cybersecurity practices to protect their mobile devices and personal information. The survey found that:

- Almost three quarters of wireless consumers reported using PINs/passwords on their smartphones, up significantly from the first survey in 2012 where only 50 percent of users reported using these features; and
- Fifty-seven percent are aware of having built-in remote lock and erase software installed on their smartphones.
- Nearly three quarters of consumers run software updates every or almost every time on their personal smartphones;
- Almost half of users responding have an anti-virus program installed on their smartphones, up 18 percent from 2015, and up 52 percent from 2012; and
- Ninety percent say they are familiar with the term cybersecurity, defining it as protection, safety and prevention of unauthorized access.

[26] http://www.capradio.org/articles/2015/10/01/experts-data-on-policing-practices-inconsistent-throughout-us/

The survey also found that only nine percent of respondents reported losing a smartphone. This is down from 13 percent last year. Of those consumers who reported having lost a device, only 20 percent reported that the device was stolen, with the rest reporting it was simply misplaced. The percentage of devices being reported as stolen, as opposed to misplaced, has decreased year over year.

Chart 1.2: Trends in Lost Devices Characterized as Stolen



As previously noted, 57 percent of smartphone owners say they have built-in capability for remote lock/locate/erase. Of those respondents who are aware of the capabilities, nearly 75 percent have enabled it.

More than 40 percent of those not enabling the anti-theft capabilities cite lack of need. Not having enough time to enable, and concern that they might accidentally lock or erase their data are among other top reasons for not enabling it. Notably, 34 percent of consumers not enabling the capabilities said that losing their phone would actually encourage them to enable the features.

4.2.2.2 Anecdotal Reports and Publicly Available Data

Since 2013, reports of mobile device thefts have shown indications of steady decline. In Washington, D.C., Metro Transit Police data show a decline of 51 percent in the theft of cell phones from 2013 to 2015.

The New York City Police Department's (NYPD) Crime Complaint database includes details about crimes related to electronic devices.[27] According to this data, thefts of personal electronic devices in New York have fallen by a third since 2013. Another survey, from 2015, found that

[27] https://www1.nyc.gov/site/nypd/stats/crime-statistics/crime-statistics-landing.page

smartphone thefts dropped as phone manufactures and carriers enabled deactivation mechanisms or "kill switches" which make lost or stolen phones unusable.[28]

4.3 Recommendations

The MDTP WG does not have sufficient or complete information related to mobile device theft nationwide. However, the MDTP WG has seen anecdotal reports and survey data that suggest a significant decline in mobile device thefts since the group's inception. Though the decline coincides with the deployment of the anti-theft voluntary commitment and the release of the Stolen Phone Checker, we note that we are not able at this point to attribute this decline to any single particular initiative or effort. The MDTP WG has worked to identify sources of law enforcement data that could be used to refresh and validate this data, but has faced challenges. As a result, the MDTP WG recommends:

a. Stakeholders, including FCC and industry, focus attention on building an enduring relationship with groups that have broad membership (e.g. IACP, Major Cities Chiefs Police Association (MCCA), National Sheriffs' Association (NSA)) to help simplify the efforts of gathering mobile device theft statistics. CTIA's Stolen Phones Working Group could be a possible point of contact outside of the TAC MDTP WG.
b. FCC consider additional methods to gather statistics related to mobile device theft. For example, the FCC could work with IACP, MCCA, or NSA to conduct a survey of members.
c. Finally, industry groups are encouraged to conduct surveys to identify consumer trends, awareness, and adoption of available security and anti-theft tools. Future surveys could expand upon the source of consumer knowledge and awareness (i.e. are consumers implementing these practices based on carrier recommendations, law enforcement public awareness campaigns, or news and consumer-oriented tips and best practices?). Determining where most consumers are obtaining information about mobile device security practices may help sharpen the focus of existing messaging, identify potential gaps in information, and enhance the most effective means of reaching end-users.

[28] Consumer Reports, *Smartphone thefts drop as kill switch usage grows* (Jun. 11, 2015) available at: https://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm.

5 International Efforts on Mobile Device Theft Mitigation

5.1 Overview

The MDTP WG was asked to engage with international counterparts and examine how mobile device theft prevention is being addressed internationally. In addition to exploring the differing approaches to device theft mitigation, the WG was tasked with exploring whether information could be obtained to help answer the question of where stolen devices end up—a question that has proven challenging to answer.

5.2 *Mobile Device Theft Mitigation in Latin America*

The MDTP WG initially focused on the Latin American region. This region was selected in part because of the focus on mobile device theft throughout the region and the many efforts already underway. In Latin America, two primary means for mitigating mobile device theft have emerged: IMEI-based blocking measures and technical solutions. For blocking measures, there are lists for both blocked devices (blacklists) and permitted devices (whitelists). Within Latin America, subscriptions to the GSMA's database rose rapidly after a 2011 resolution by the Inter-American Telecommunications Commission (CITEL) promoting measures to fight device theft.[29] CITEL is comprised of governmental representatives and associate members from industry.

Latin America has so far focused primarily on a combination of blacklisting and whitelisting to attempt to curb mobile device theft, with little effort to promote technical solutions. As discussed above, manufacturer-led technical approaches to deter and prevent theft, such as "kill switches" and CTIA's Smartphone Antitheft Voluntary Commitment, have been shown to make a significant impact on the rate of device theft.[30] These solutions are generally available to smartphone users worldwide, either directly from manufactures or through the internet as downloadable applications. However, while these solutions have been publicized widely throughout the United States, there has been little high-profile support or consumer education efforts for such technical solutions throughout Latin America.[31] As a result, consumer adoption of such technical solutions may be lacking in Latin America.

[29] *See* Telecommunications Management Group, Inc, *Mobile Device Theft in Latin America*, 7 (Nov. 2017).
[30] *See id.* at 13.
[31] *Id.* at 14-15.

5.3 *MDTP WG Engagement*

The MDTP WG specifically met with representatives from Colombia, Peru, Costa Rica, and Brazil. Members of the WG joined the FCC in several telephone conversations and one in-person meeting. These discussions provided an opportunity to share experiences and insight into mobile device theft in the respective countries.

The approach to combatting mobile device theft throughout these countries largely mirrors the efforts of the broader region and consists of a combination of whitelisting, blacklisting, and regulations. The focus in recent years has been on network-level solutions, as opposed to implementing device-based antitheft tools for device users, although some countries such as Brazil and Colombia have been considering technical solutions such as the "kill switch." As seen in the chart below, each of the countries has implemented blacklisting and most have implemented whitelisting.

The countries also discussed challenges. All of the countries highlighted challenges with IMEI security among their primary issues, as this decreases the effectiveness of blacklisting capabilities. IMEI integrity is an issue that this WG has explored in the past.[32] For reasons unknown at this time, interviews conducted by the WG suggest that IMEI security is not a significant problem in the United States compared to that reported by the Latin American countries engaged in the WG outreach.

Table 1.2: County Approaches to Mobile Device Theft Mitigation

Country	Blacklist	Whitelist	Challenges
Colombia	Yes	Yes	IMEI Tampering
Peru	Yes	Yes	Flashing IMEIs
Brazil	Yes	Yes - Pilot Program	IMEI Tampering
Costa Rica	Yes	No	IMEI Security – Focusing on a solution that will allow blocking

[32] *See* Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) Analysis and Recommendations, 38-41 (Dec. 4, 2015).

			from the network while also allowing roaming. Slow response times. Currently takes 24 hours to refresh the lists, would like to have that down to 15 minutes.

5.4 *Efforts to Trace the Path of Stolen Devices*

Tracing the movement of devices once they are stolen can be a challenge. As reported in an earlier report produced by the MDTP WG, the relationship between mobile phones, subscribers, and operators makes this difficult to track.[33]

The MDTP WG observes that broader international efforts are essential to stemming mobile device theft. Mobile device theft is "an intrinsically transnational issue as stolen phones can be moved easily across borders to avoid detection, often being connected to organized crime."[34] Given this, the MDTP WG attempted to obtain information during our conversations that would assist with identifying where devices stolen in the United States go. Most of the countries expressed an interest in attempting to locate and share data on this point, but as of today, the MDTP WG has not obtained any additional information.

In Latin America, as of 2017, 64 of 87 operators were connected to GSMA's IMEI database and regional efforts were launched to better coordinate efforts. However, while there is some regional coordination in the fight against device theft (*e.g.* efforts by CITEL and others) with laws and policies enacted on a national level, the result is a complicated web of varying systems which approach the same issue in different ways. Further, not all operators in the region utilize

[33] *See* Technological Advisor Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) Evaluation of Theft Prevention Measures, 24-28, (Dec. 2017).
[34] *Id.* at 19.

the database in the same way, creating inconsistencies in the availability and usefulness of information.[35]

In "Latin America…each country takes a slightly different approach. While certainly intended to address what policymakers and regulators view as solutions tailored to their countries' needs, the result is a patchwork of policies and approaches that creates difficulties with respect to harmonization and data sharing."[36]

Unlike the United States, which has encouraged voluntary, industry-led approaches that have established coalitions and widely adopted practices to protect consumers, an overly prescriptive framework, such as that in Latin America, can actual complicate and stymie efforts to mitigate mobile device theft. This holds especially true when coordinating information sharing efforts on a global scale.

5.5 ***Recommendations***

As discussed above, the WG and FCC staff participated in discussions with representatives from several countries in the Latin America region—Costa Rica, Brazil, Peru, and Colombia. In these discussions, each of the countries interviewed identified IMEI duplication as a primary concern. As a result, the MDTP WG encourages FCC staff to:

a. Request and review evidence from international counterparts to assess differences internationally—including the prevalence of substandard and counterfeit devices in local markets—that make IMEI duplication a problem abroad and not a problem domestically;
b. Continue to engage with South American counterparts on mobile device theft issues relating to collaboration on the global blacklist database; country specific concerns, such as duplicate IMEIs and issues related to whitelisting; international trafficking of stolen devices; and sharing best practices and improving cross-border coordination;
c. Continue to promote and expand awareness and use of the GSMA Black List, IMEI security weakness reporting and correction enablers, and device-based anti-theft features internationally; and
d. Continue to study the movement of stolen devices from the U.S. to other jurisdictions and use that information to encourage other countries to adopt measures to combat the import and use of devices stolen abroad.
e. Work with relevant standards organizations (e.g. ATIS) and industry associations such as GSMA, which operates an IMEI security monitoring and

[35] *See* Telecommunications Management Group, Inc, *Mobile Device Theft in Latin America*, 19-21 (Nov. 2017).
[36] *Id.* at 22.

reporting service to assess mobile device IMEI security levels and the availability of hacking tools, to better understand security of IMEI and why IMEI reprogramming is reported as a major source of fraud in foreign countries.

6 Summary and Conclusion

Experience in the last several years has demonstrated that customer actions to secure mobile devices against theft are dependent upon both ease-of-use of security features as well as the customer perception of the value of information stored on the phone. While significant progress appears to have been made in the U.S., recent discussions with Latin American countries has indicated that misuse of mobile devices remains a significant issue both in their respective countries as well as inter-country. Future efforts should be focused on working with interested international regulatory authorities in understanding the problem, sharing best practices, and cooperating on methods to combat illegal use of mobile devices.

Appendix A: Glossary

FCC	**Federal Communications Commission**
GSMA	**GSM Association**
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.
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.