

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Report of Technological Advisory Council)	ET Docket No. 14-143
Subcommittee on Mobile Device Theft)	
Prevention)	

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Thomas C. Power
Senior Vice President, General Counsel

John A. Marinho
Vice President, Technology and Cybersecurity

Jamie A. Hastings
Vice President, External and State Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200

January 30, 2015

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND SUMMARY	1
II. INDUSTRY HAS BEEN ACTIVELY ADDRESSING SMARTPHONE THEFT.	3
III. THE WIRELESS ECOSYSTEM, LAW ENFORCEMENT AND CONSUMERS MUST CONTINUE TO COLLABORATE AND BUILD ON EXISTING SUCCESSES.	7
IV. THE FCC SHOULD PROMOTE A COMMON NATIONAL FRAMEWORK WITH A COLLABORATIVE, VOLUNTARY, INDUSTRY-LED APPROACH.	9
V. THE PUBLIC NOTICE EXTENDS BEYOND THE TAC REPORT’S FOCUS ON SMARTPHONES.	11
VI. THE PUBLIC NOTICE’S INQUIRY INTO DEVICE IDENTIFIERS, DATABASE USE, AND INFORMATIONAL ISSUES CONFIRM THE NEED FOR BROAD ENGAGEMENT ON MULTI-LAYERED SOLUTIONS.	13
A. The integrity of device identifiers (and any future alternative) depends on multiple, global stakeholders.	13
B. Improving the timeliness, accuracy and availability of data about smartphone theft for use by law enforcement requires effort by the FCC, law enforcement and consumers as well as industry.	15
C. The U.S. mobile industry strives to ensure that lost or stolen devices are not placed into service on U.S. networks and will continue to do so.	17
VII. CONCLUSION.....	18

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
Report of Technological Advisory Council) ET Docket No. 14-143
Subcommittee on Mobile Device Theft)
Prevention)

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® (“CTIA”) submits these comments in response to the Commission’s Public Notice (“PN”),¹ seeking input on recommendations contained in the FCC’s Technological Advisory Council (“TAC”) Subcommittee on Mobile Device Theft Prevention December 4, 2014 Report (the “TAC Report”).² CTIA shares the FCC’s concerns about smartphone theft, as is evidenced by the significant steps that the industry has already taken to educate consumers and give them and law enforcement the tools they need to address the issue. Smartphone theft is a global challenge, with solutions requiring action and collaboration by law enforcement, industry, regulatory agencies, and consumers. The TAC Report details the actions of the stakeholders, and noted that progress is being made.

For its part, the wireless industry has been using its expertise in device and system design to refine multi-layered solutions. As explained below, the industry has been leading with innovative solutions and extensive consumer education efforts. This includes our industry’s

¹ *Comments Sought on Technological Advisory Council Report on Mobile Device Theft Prevention*, Public Notice, DA 14-1828 (rel. Dec. 12, 2014) (“PN”).

² Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP), Version 1.0 (Dec. 4, 2014), *available at* <http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf> (“TAC Report”).

2014 Voluntary Commitment³ to produce and offer consumers, at no cost, an antitheft solution, and ongoing consumer educational efforts and the April 2012 agreement to integrate the GSM Association (“GSMA”) stolen phone database.

CTIA and its members contributed to the TAC Report and appreciate its comprehensive, data-driven approach to identifying and addressing the particular problem of smartphone theft. The report is timely, as many states have been considering and enacting their own technical mandates, and the 2014 Voluntary Commitment is being implemented by July 2015. The TAC Report offers 33 recommendations for the FCC, law enforcement, and industry to consider and act on in the future. A primary recommendation is that the FCC pursue a common national framework for smartphone anti-theft measures. Many recommendations are aimed at raising awareness of existing solutions to smartphone theft and gathering more information about their effectiveness. Others intend to ensure that all stakeholders—law enforcement, regulatory agencies, carriers, OEMs, OS providers, resellers, and consumers—play their part.

The next steps are important. The TAC Report provided a solid roadmap, in particular the call for a common national framework. A common national approach is key to preventing consumer confusion and market fragmentation, which would be the result of multiple state regimes. The TAC Report reflects a consensus that solutions involve the entire mobile ecosystem, including the FCC and the public safety community. Duplicative or conflicting efforts threaten unnecessary costs and burdens, to the detriment of consumers and could unintentionally inhibit our collective anti-theft efforts.

³ CTIA, *Smartphone Anti-Theft Voluntary Commitment* (rel. Apr. 15, 2014), available at <http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment> (“2014 Voluntary Commitment”).

The TAC Report rightly contemplates a leadership role for the FCC. The Commission can use its technical expertise as it facilitates stakeholder involvement, particularly consumer engagement and the creation of task forces with law enforcement. The TAC Report recommends several activities in which CTIA looks forward to participating. The FCC can and should seek input on those activities. Yet given the many steps suggested by the TAC, the issues raised by this PN were surprising. Though the TAC Report limited its scope to smartphone theft, the PN seeks comment on the functionality for *all* mobile wireless devices. This expansion may distract the FCC and the wireless ecosystem from the task at hand, which is to take action on smartphone theft. The PN's other questions about International Mobile Equipment Identity ("IMEI") integrity and carrier action to improve databases, when viewed in isolation, may shift stakeholder focus away from the TAC Report's emphasis on engagement by the entire ecosystem.

Based on the TAC Report, trends are headed in the right direction.⁴ The best way to build on this success is to continue to involve the entire ecosystem, retain flexibility, and avoid disparate requirements that increase regulatory burdens and consumer confusion. The TAC Report rightly stresses that there is no "silver bullet" solution to smartphone theft and proposes a multi-layered, global approach. The TAC Report's recommendations should be pursued in concert with law enforcement, technical experts, and consumers.

II. INDUSTRY HAS BEEN ACTIVELY ADDRESSING SMARTPHONE THEFT.

The wireless industry has been actively addressing smartphone theft through innovation and technology, education and collaboration. The TAC Report recognizes that "[t]here exists a

⁴ See TAC Report at 7, 26-27, 37-42, 95-134.

wealth of industry existing solutions that the mobile industry offers today as well as recent industry announcements that highlight ongoing enhancements.”⁵

The industry drew on its expertise and collaborated to pioneer a voluntary approach to smartphone theft in 2014. Numerous device manufacturers (“OEMs”) and wireless carriers signed CTIA’s 2014 Voluntary Commitment pledging that smartphones first manufactured after July 2015 will pre-load or offer for download a free, baseline anti-theft tool. The tool provides the connected capability to: (1) remotely wipe the authorized user’s data, such as contacts, photos, and emails, on the smartphone in the event it is lost or stolen; (2) render the smartphone inoperable to an unauthorized user, except in accordance with Commission rules for 911 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; and (4) reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible, such as from the cloud.⁶ In addition to the baseline tool, industry has apps that can locate, lock and/or erase a lost or stolen smartphone. OEMs, carriers, and third parties have been working on solutions, and innovation continues.

The 2014 Voluntary Commitment builds upon the April 2012 agreement between CTIA, the FCC, and law enforcement (the “2012 Agreement”) to develop steps to help deter smartphone thefts and protect consumer data.⁷ As a result of the 2012 Agreement, wireless

⁵ *Id.*, at 41.

⁶ *Id.*

⁷ FCC, *FCC Chairman Genachowski Joins Senator Schumer, D.C. Mayor Gray, State Police Departments, and Wireless Carriers to Announce Initiatives to Combat Massive*

carriers completed their commitment to use the GSMA Global IMEI Database in November 2013 to report and track stolen 4G/LTE phones. The database allows wireless carriers to deny network service if the database shows a device as lost or stolen and it provides a meaningful resource for law enforcement to deter thefts. Moreover, as additional carriers integrate with the GSMA Global IMEI database, carriers can share data and ensure that a device blocked on one network cannot be used on other networks. To enhance their effectiveness, U.S. databases integrate internationally, and efforts are underway to link more foreign carriers and countries to the database to mitigate the export of stolen phones. The Commission could play an important role in supporting this effort with its counterparts in other countries to enhance the effectiveness of the global database.⁸

Industry knows from these efforts that consumers are key to mobile security. This is why industry has engaged in numerous educational activities, as contemplated in the 2012 Agreement, urging consumers to be aware of their surroundings and use passwords, apps and other security measures. Industry works to educate consumers by providing guides for best practices to secure and protect personal data in the mobile environment.⁹ Advice covers security at every stage, from configuring devices, to checking permissions and understanding the security (or lack of) found on different types of networks. It also covers how to protect personal data in the event a device is lost or stolen. Each element of the industry plays a role in educating

Smartphone & Data Theft (Apr. 12, 2012), available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-313509A1.pdf.

⁸ See TAC Report Recommendation 1.13.

⁹ See CTIA, *Today's Mobile Cybersecurity: Protected, Secured and Unified*; CTIA, *Today's Mobile Cybersecurity: Blueprint for the Future*; CTIA, *Today's Mobile Cybersecurity: Industry Megatrends & Consumers*; CTIA, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*; CTIA, *Today's Mobile Cybersecurity: Information Sharing*.

consumers. Platform providers and application developers work to make loading of applications and software permissions more intuitive and easier to understand, and manufacturers provide information, both on the device and in user guides and online, to help consumers protect their devices straight out of the box. Likewise, many U.S. carriers have websites, tips, and customer service numbers where customers can address lost or stolen phone issues. CTIA amplifies all these efforts by making educational information available online, including consumer tips, FAQs,¹⁰ and a public service announcement video.¹¹ Industry efforts also include law enforcement. For example, CTIA has provided police stations nationwide business card-sized tips to share with their citizens.¹²

These efforts parallel global initiatives through GSMA. In 2012, the GSMA North America (“GSMA-NA”) Fraud Forum and Security Group Stolen Handset Task Force published its “Analysis and Recommendations for Stolen Mobile Device Issue in the United States.” The report identified tools for wireless operators to respond to law enforcement requests to address stolen handsets, identified methods for operators to deny service to reported stolen devices, and identified how to share the IMEI of the stolen mobile devices among wireless operators.

¹⁰ See CTIA, *How to Deter Smartphone Thefts and Protect Your Data*, available at <http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data>; CTIA, *FAQ on Lost/Stolen Devices*, available at <http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/faq-on-lost-stolen-devices>; CTIA, *Cybersafety Tips*, available at <http://www.ctia.org/your-wireless-life/consumer-tips/tips/cybersafety-tips>.

¹¹ See CTIA, *CTIA Releases Public Service Announcement Video to Help Educate Consumers on How to Protect Themselves if Their Smartphones are Lost or Stolen*, available at <http://www.ctia.org/resource-library/press-releases/archive/ctia-the-wireless-association-releases-public-service-announcement-video-to-help-educate-consumers-on-how-to-protect-themselves-if-their-smartphones-are-lost-or-stolen>

¹² See CTIA, *Deter Smartphone Theft NOW*, available at <http://www.ctia.org/docs/default-source/default-document-library/theft-business-cards.pdf>

CTIA agrees with the TAC that “[o]ver the past few years, great strides forward have occurred regarding technology methods to reduce phone theft via solutions voluntarily rolled out by carriers, OS providers, manufacturers and third party vendors” and that “[t]his is a very good start and there is some evidence it is impacting criminal activity even today.”¹³ Industry fulfilled the 2012 Agreement, contributes to the GSMA database and proactively educates consumers. Industry participants are on schedule to meet the 2014 Voluntary Commitment. We are implementing these initiatives, which will evolve as technological innovation continues, consumer behavior changes and stakeholder participation increases.

III. THE WIRELESS ECOSYSTEM, LAW ENFORCEMENT AND CONSUMERS MUST CONTINUE TO COLLABORATE AND BUILD ON EXISTING SUCCESSES.

CTIA has long said that combating stolen cellphones will require a comprehensive, global effort. CTIA supported federal legislation introduced to impose tough penalties on those who steal devices or modify them illegally, to help dry up the market for those who traffic in stolen devices.¹⁴ And CTIA emphasizes that more countries need to participate in the global stolen phone database to prevent criminals from selling devices internationally.¹⁵

All sectors of the global wireless ecosystem must work together to promote smartphone security. The mobile environment is a complex, global, and interrelated “system of systems.”

¹³ TAC Report, at 7.

¹⁴ CTIA, *CTIA Statement on the Mobile Device Theft Deterrence Act* (May 14, 2013), available at <http://blog.ctia.org/2013/05/24/theft-deterrence-act/>. CTIA agrees with the TAC Report that “smartphone theft is an international issue which will ultimately require multi-national coordination.” TAC Report, at 6.

¹⁵ Testimony of Jamie Hastings, CTIA, Regarding A 3157, Before the New Jersey Assembly Consumer Affairs Committee (Oct. 2, 2014), available at <http://www.ctia.org/docs/default-source/Legislative-Activity/ctia-letter-in-opposition-to-new-jersey-a-3157-regarding-stolen-phones-issues.pdf?sfvrsn=0>.

The TAC Report recognizes that “mobile device theft is a complex issue that is present on both local and global level[s]” and that “[s]martphone anti-theft deterrence has many aspects, including wireless operator network-based solutions, use of global databases, and device-based solutions.”¹⁶

Likewise, no one element of the market can solve this problem alone. The TAC Report makes clear that “a multilayered solution is most likely to be effective.”¹⁷ In discussing software-, hardware-, and network-based approaches, the Report states that

“[i]t is important to note that many solutions are systemic in nature and may use all of the above three categories in some fashion. Each one of the above categories addresses different aspects of security and each one adds key functionality since no one category alone is comprehensive. In this scenario the different category elements work collaboratively and provide enhanced security.”¹⁸

Critically, the TAC Report acknowledges that successful solutions must extend beyond the global wireless industry to include government and consumers. The TAC Report suggests that the key role the Commission can and should play is as a convener. For instance, the Report recommends that the FCC should seek input from consumer organizations, reach out to major law enforcement groups, engage international counterparts, and work with CTIA and GSMA-NA to encourage additional operation participation in the 2012 Agreement.¹⁹ There are many tasks for the FCC, and CTIA looks forward to assisting the FCC in these important activities.

¹⁶ TAC Report, at 6, 8.

¹⁷ *Id.*, at 18.

¹⁸ *Id.*, at 46.

¹⁹ *See id.*, at 70-74.

The Report identifies critical law enforcement and consumer stakeholders. Given the benefits of emerging solutions, it is unfortunate that not all consumers take advantage of them.²⁰ Similarly, the TAC Report notes that law enforcement may not be aware of the importance of device identifiers, or their ability to access helpful information.²¹ There is more to be done; consumer and public education will continue to be vital. Therefore, CTIA supports the Report’s recommendations to engage consumers and law enforcement so that they can better use existing solutions and so that the ecosystem can gather additional information, which will enable us to refine and improve solutions.²² We also support the TAC Report’s recommendations on education, because as the TAC concludes, “there is no single technology ‘silver bullet’ that will eliminate phone theft.”²³

IV. THE FCC SHOULD PROMOTE A COMMON NATIONAL FRAMEWORK WITH A COLLABORATIVE, VOLUNTARY, INDUSTRY-LED APPROACH.

CTIA agrees with the TAC Report’s key recommendation that the FCC should “[e]stablish a common national framework for smartphone anti-theft measures that considers all stakeholders and input from all parties involved and explore the basis for preemption.”²⁴ The framework should be developed in cooperation with industry. The TAC Report reflects this by recognizing that the most effective way to address smartphone theft will be a collaborative effort with industry, consumers, the Commission and law enforcement working to produce a voluntary, flexible, unitary framework. CTIA agrees that “it is important that the FCC provide national

²⁰ See *id.*, at 25-26.

²¹ See *id.*, at 43.

²² *Id.*, at 70-74.

²³ *Id.*, at 7, 52-54.

²⁴ *Id.*, at 7.

leadership in addressing this critical global issue.”²⁵ The agency is an ideal convener of industry participants, federal agencies, state and local law enforcement, consumer groups, and international interests. A unified national framework would draw on the FCC’s expertise and authority over the field of radio transmissions, devices, and the technical and operational aspects of wireless service. A unified national framework also would address the desire of some state and local governments to enact their own requirements and provide predictability to the ecosystem charged with developing solutions. In particular, divergent state approaches conflict with federal law and policy and undermine the uniform national approach to wireless service that has been a driver of growth and innovation. The TAC Report acknowledges that a national framework would “prevent conflicting or growing requirements that may impact the ability of the industry to deliver solutions uniformly to consumers in the United States and US territories in a timely manner.”²⁶ The FCC should move quickly to promote a national framework for smartphone anti-theft measures, particularly given the 2015 compliance deadlines in existing state laws and pending bills in other legislatures.²⁷ The common national framework should give States comfort that consumers are protected and solutions are implemented. CTIA agrees with the TAC Report that divergent bills from state and local governments would “result in significantly different requirements for devices between states and could require devices to be

²⁵ TAC Report, at 6.

²⁶ *Id.*

²⁷ *See id.*, Appendix B (Minnesota law), Appendix C (California law), and Table 5: Planned State Laws.

manufactured uniquely for each state.”²⁸ It is not tenable to have “50 different and potentially inconsistent state laws as states struggle with the mobile device theft issue.”²⁹

Divergent state “kill switch” requirements would lead to consumer confusion and needlessly impose cost. Compliance with 50 different state technical mandates and reporting obligations, together with needed efforts to educate consumers about different regimes, would increase the cost of devices and service. Consumers have come to rely on a unified, national approach to wireless services, particularly regarding technical and operational issues, including public safety functions like 911. Consumers do not expect that state political boundaries will affect the function and operation of their smartphones, nor should they come to expect such balkanization. Most customers would not anticipate that a smartphone purchased in an airport in Minnesota during a layover could have different safety and security functionality than one purchased in the consumer’s home state of Oregon or their destination in Illinois.

In sum, a unitary, voluntary framework will spur effort to advance smartphone security and avoid consumer confusion and costly, duplicative or conflicting requirements.

V. THE PUBLIC NOTICE EXTENDS BEYOND THE TAC REPORT’S FOCUS ON SMARTPHONES.

The PN inquires about “[m]aking ‘lock/wipe/restore’ functionality operational by default on all mobile wireless devices.”³⁰ Based on the TAC Report itself, this inquiry is premature and could divert resources from the problem identified in the TAC Report.

Comprehensive and ambitious, the TAC Report focuses on the identified challenge of smartphone theft, in order to focus participants’ efforts and ensure it had adequate data. The

²⁸ *Id.*, at 34.

²⁹ *Id.*, at 44.

³⁰ PN, at 1.

Report states: “The scope of this report is the theft of smartphones. Any reference to mobile devices, mobile phones, cellular phones in this report can be considered to be a reference to smartphones.”³¹ In Section 1.3, the TAC Report repeats:

“The scope of this report has purposefully been limited to the theft of smartphones since smartphones are by far the largest component of the problem and is sufficient (sic) complex as a topic of focus. Any references to mobile devices, mobile phones, cellular phones in this report can be considered to be a reference to smartphones.”³²

The PN seeks comment on a broader issue, exploring antitheft functionality for “all mobile devices.” The range of products in this category – including tablets, personal computers, basic mobile phones, personal health devices (i.e. Fitbit), wearable technology, and others – goes well beyond the data and challenge considered in the TAC Report. As the TAC Report acknowledges, “to truly understand the issue of smartphone crime, accurate data must be provided.”³³ No data has been provided on theft of non-smartphone mobile devices, so the TAC Report provides scant basis for commenters to evaluate the issue. Given the nature of the TAC Report, industry experts within the TAC would be in the best position to assess in the first instance important questions regarding the utility and compatibility of anti-theft solutions beyond smartphones. This includes considering whether the problem of smartphone theft manifests itself the same way across other mobile devices and what solutions, if any, may be appropriate. The TAC Report acknowledges this, as part of its recommendations.³⁴

³¹ TAC Report, at 6.

³² *Id.*, at 9.

³³ *Id.*, at 22.

³⁴ *See, e.g., id.* at 74 (recommending future work in the TAC to study new risks and the changing threat environment). By choosing to focus this Report on smartphone theft, one category of mobile device theft, the TAC left broader questions to future effort.

Therefore, it is not prudent to expand the inquiry before smartphone solutions have matured and been more widely adopted. Adding more device categories may increase the complexity of solving the problem identified in the smartphone market and will dilute finite resources. The FCC should concentrate on the problem identified by the TAC before expanding its focus.

VI. THE PUBLIC NOTICE’S INQUIRY INTO DEVICE IDENTIFIERS, DATABASE USE, AND INFORMATIONAL ISSUES CONFIRM THE NEED FOR BROAD ENGAGEMENT ON MULTI-LAYERED SOLUTIONS.

A. The integrity of device identifiers (and any future alternative) depends on multiple, global stakeholders.

The PN seeks comment on “[e]nhancing protection of unique mobile wireless device identifiers ([IMEI and MEID numbers] or perhaps a new identifier to be developed) from alteration.”³⁵ Industry is addressing identifier integrity, which is a global challenge. Indeed, activity around device identifiers must involve the global wireless ecosystem, as well as law enforcement.

As an initial matter, the TAC Report focuses broadly on how to expand the utility of *existing* identifiers through databases and other ways to ensure that lost or stolen smartphones are not readily usable. A fundamental challenge has been a lack of awareness of the importance of device identifiers. This is why the TAC Report includes recommendations to improve awareness about IMEI/MEID and device identifiers’ role in efforts to combat smartphone theft.³⁶ Such education rightly focuses on law enforcement and consumers.

³⁵ PN, at 1.

³⁶ See, e.g., TAC Report Recommendations 2.2, 3.6.

Because protecting identifiers relates to the use of databases and overall smartphone security, the TAC Report noted the desirability of ensuring identifier integrity, which requires engagement throughout the global mobile ecosystem. For example, the TAC Report explicitly notes that “[a] comprehensive technology solution” for addressing smartphone theft “does not involve a single solution, but will require solutions across networks and devices.”³⁷ IMEI and MEID integrity primarily are the responsibility of OEMs, so solutions for enhanced protection must be seen in the context of the global wireless ecosystem. The TAC Report noted the challenge posed by counterfeited devices and observed that, “[w]hile all smartphones sold in reputable US retail environments support” GSMA’s principles to strengthen IMEI security, there have been obstacles to global adoption.³⁸

Despite the challenges of a global system, industry is addressing IMEI integrity. The TAC Report recognizes that the world’s leading GSM/LTE device manufacturers agreed to support guidance that the GSMA has produced: “Security Principles Related to Handset Theft” for GSM, UMTS, and LTE devices.³⁹ The Security Principles are “a range of measures to strengthen IMEI security to provide confidence in device blocking and the deployment of enabling technologies and progress” which are monitored by the GSMA.⁴⁰ The Security Principles set forth criteria for improved regional theft deterrence and handset security, including internal resource integrity, access control and partitioning for handset applications and software,

³⁷ TAC Report, at 69.

³⁸ *Id.*, at 7.

³⁹ *Id.* (citing GSMA, *Security Principles Related to Handset Theft* (2012), available at <http://www.gsma.com/publicpolicy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf> (“GSMA Security Principles”))

⁴⁰ *Id.*, at 7.

and software quality.⁴¹ And as the Security Principles make clear, “[t]he GSM Association is undertaking a concerted drive to extend the use of Equipment Identity Registers (CEIR & EIR) across the global GSM operator community to ensure stolen handsets can be barred from networks by using the handsets’ IMEI numbers.”⁴² Importantly, the Security Principles “do not propose to mandate a standardised way to achieve IMEI integrity,” but instead “set out handset security principles to provide guidance to handset manufacturers and to provide operators with a set of high level criteria against which handset security can be assessed.”⁴³

The FCC should avoid any effort that would stifle or homogenize ongoing efforts to improve the protection of unique smartphone identifiers.

B. Improving the timeliness, accuracy and availability of data about smartphone theft for use by law enforcement requires effort by the FCC, law enforcement and consumers as well as industry.

The PN inquires about the TAC Report’s recommendations to industry for “improving the timeliness, accuracy and availability of data about mobile wireless device theft for use by law enforcement.”⁴⁴ CTIA and its members support efforts to meet this goal, which require input from many stakeholders over time.

As the TAC Report noted, not all law enforcement agencies make optimal use of information already available. In its Gap Analysis, the TAC Report concluded, among other things, that “law enforcement officers are not fully aware of how to access information that is in

⁴¹ GSMA Security Principles, at 5-9.

⁴² *Id.*, at 4.

⁴³ *Id.*, at 4-5.

⁴⁴ PN, at 1.

the GSMA IMEI Database” or about third-party databases.⁴⁵ Recognizing this, the TAC Report’s varied recommendations were directed to many stakeholders, including law enforcement and the FCC. In particular, several key recommendations focused on law enforcement, including that a single point of contact serve as a clearinghouse for information and that an education campaign be developed with help from CTIA and others.⁴⁶ Industry can and does provide information and assistance, will participate in these efforts, and is confident that they will continue to yield dividends. Additionally, CTIA supports the TAC Report recommendations to CSRIC and ATIS regarding their efforts to develop standards-based efforts to improve law enforcement access to handset identifiers.⁴⁷

Further, as explained above, consumer awareness remains critical. As the TAC notes, “consumers are more likely to report their devices lost/stolen as awareness of the blacklisting capability increases.”⁴⁸ CTIA supports Recommendation 3.6 “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.”⁴⁹ This includes cited efforts to raise IMEI awareness, such as urging consumers to “find the IMEI or MEID number on your mobile device,”⁵⁰ and encouraging consumers to report device theft to law enforcement and carriers. CTIA also supports the TAC’s suggestion that the FCC “promote greater consumer awareness of

⁴⁵ TAC Report, at 43.

⁴⁶ See TAC Report Recommendations 2.1, 2.2.

⁴⁷ See TAC Report Recommendations 1.4, 1.5.

⁴⁸ TAC Report, at 26.

⁴⁹ TAC Report Recommendation 3.6.

⁵⁰ TAC Report, at 51.

existing anti-theft measures,” using social media, blogs, outreach to other agencies, and the Consumer Advisory Committee.⁵¹

At bottom, improving the availability of databases – and the information in them – is a virtuous cycle. Awareness and collaboration foster additional reporting, thereby increasing use of the databases, which encourages more reporting, and so on.

C. The U.S. mobile industry strives to ensure that lost or stolen devices are not placed into service on U.S. networks and will continue to do so.

The PN asks what steps would need to be taken by the mobile wireless communications sector to ensure that devices “placed into service on networks in the United States have not been listed as lost or stolen on relevant databases.”⁵²

Industry efforts, the TAC Report, and these comments confirm that the long-term solution to smartphone theft does not rely exclusively on carriers looking up devices on blacklists. Stopping smartphone theft requires engagement by all stakeholders, including local law enforcement, resellers, and consumers. Awareness and innovative solutions can reduce theft in the first place. Preventing the use of stolen devices through list lookups is improving, and will continue through education, awareness, technological innovation, and information-sharing.

The TAC Report acknowledges that the largest U.S. carriers “have invested in the network infrastructure necessary to block devices on their networks and they act on reports of device loss/theft from their customers by placing the device identities on a blacklist, which ensures that the devices are blocked on the home network.”⁵³ Additionally, “because the carriers

⁵¹ TAC Report Recommendations 1.14, 1.16, 1.17.

⁵² PN, at 1.

⁵³ TAC Report, at 34.

share data through the global GSMA IMEI Database, the blocking of a device on one network becomes effective on the other technology specific networks.”⁵⁴

CTIA supports the TAC Report Recommendation 1.15 that it work with the FCC and GSMA-NA to encourage additional participation with the April 2012 Voluntary Commitment, including database and network solutions.”⁵⁵ CTIA also supports the TAC Report Recommendation 3.4 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.”⁵⁶

VII. CONCLUSION

CTIA appreciates the FCC’s effort to draw attention to a problem that industry has been addressing. Disparate state approaches are not the answer. Instead, FCC leadership to facilitate broad engagement and awareness will promote a virtuous cycle: empowered consumers will take advantage of existing and developing solutions to protect their device and report loss or theft. Law enforcement will have greater awareness and access to increasingly robust tools and information. Industry will refine technical solutions that empower consumers and, in turn, make more information available to law enforcement and databases. These efforts will improve our ability to ensure that unauthorized users cannot take advantage of the national wireless network. With leadership by the FCC to promote a voluntary, collaborative approach, we expect smartphone theft to continue to decline.

No one piece of the puzzle can be overlooked. All of these steps complement each other to reduce the incentive and ability to steal smartphones. Technology and education already are

⁵⁴ *Id.*, at 34-35.

⁵⁵ TAC Report Recommendation 1.15.

⁵⁶ *Id.*, Recommendation 3.4.

bearing fruit, in observed reductions in smartphone theft, as the TAC Report noted. CTIA and its members look forward to helping the FCC, law enforcement and consumers act on the many important recommendations in the TAC Report.

Respectfully submitted,

By: /s/ John A. Marinho

John A. Marinho
Vice President, Technology and Cybersecurity

Thomas C. Power
Senior Vice President, General Counsel

Jamie A. Hastings
Vice President, External and State Affairs

CTIA – The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 736-3200

Dated: January 30, 2015