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

In the Matter of	)	
	)	
COMMENT SOUGHT ON	)	
TAC SUBCOMMITTEE ON	)	**ET DOCKET**
MOBILE DEVICE THEFT	)	**NO. 14-143**
PREVENTION RECOMMENDATIONS	)	
	)	
	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA") hereby submits comments to the Federal Communications Commission ("Commission") in the above-captioned proceeding.[1] TIA appreciates the opportunity to address the Report ("Report") of Technological Advisory Council (TAC) Subcommittee (Subcommittee) on Mobile Device Theft Prevention.[2] The Subcommittee should be commended for its very thorough report, meeting its mandate "of exploring the problem of mobile

[1] *See*, Comment Sought on TAC Report on Mobile Device Theft Prevention Recommendations, DA 14-1828 (Rel. December 12, 2014) ("Public Notice" or "PN")

[2] *See,* Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) Version 1.0, December 4, 2014 ("Report") http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf

device theft and developing industry-wide recommendations for the FCC to deter and mitigate mobile device theft."

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence, and world-wide environmental regulatory analysis. Its hundreds of member companies manufacture or supply the products and services used to provide broadband and broadband-enabled applications. Since 1924, TIA has enhanced the business environment for broadband, mobile wireless, information technology, networks, cable, satellite, and unified communications. TIA's standards committees create consensus-based voluntary standards for numerous facets of the ICT industry.

II. MANDATING DEVICE FUNCTIONALITY

A. A National Approach

TIA supports establishing a single common national framework for smartphone anti-theft measures and strongly encourages the Commission to explore the basis for Federal preemption.[3] The marketplace fragmentation in which multiple local approaches co-exist would undermine a key policy goal for the Commission to make devices more affordable. As noted by the Subcommittee, economies of scale provide the most efficient distribution of anti-theft measures throughout the base of users.

[3] *See,* Recommendation 1.1: The FCC TAC recommends that the FCC establish a common national framework for smartphone and antitheft measures and explore the basis for preemption. Report at p. 69

More importantly, consumers benefit from having a simple and uniform process to quickly report a stolen mobile telephone. Diverse requirements that vary from jurisdiction to jurisdiction would both undermine industry's ability to deliver solutions uniformly to consumers and be an unnecessary source of customer confusion.

B. Device Scope

The Subcommittee explicitly limits the scope of its work "to the theft of smartphones since smartphones are by far the largest component of the problem and is sufficient complex as a topic of focus. Any references to mobile devices, mobile phones, cellular phones in this report can be considered to be a reference to smartphones."[4]

TIA concurs with this focused approach. However caution should be exercised regarding the potential unintended consequences of using conclusion about smart phones that might have collateral impact on other devices, such as tablets, e-readers, gaming consoles and laptops. A clear distinction should be drawn with these other electronic devices and commercial mobile radios.

C. Technology Neutrality

TIA supports the Subcommittee's recommendation that the Commission remain: "technology neutral in any common national framework pertaining to mobile device theft prevention, allowing the industry to identify and evolve the technical approaches for solutions to meet the functional

[4] *See*, Report 1.3 Scope at p.9

requirements for smartphone anti-theft capabilities without limiting innovation by solution providers in a competitive market.'[5]

The Report extensively details a variety of solutions which have been integrated into mobile devices and their supporting systems. These solutions are consistent with device functionality and contain interfaces that will be familiar to users. TIA supports encouraging this flexibility, rather than imposing technology mandates. To reinforce the point, the following will highlight various manufacturer and third party approaches, as contained in the report:

- Apple's Find My iPhone is built into iOS and is part of a user's iCloud account. Once a user's device is enrolled, a user can log into either iCloud.com or the Find My iPhone app to remotely locate their device, play a sound on it, put it in lost mode, or securely erase it remotely – and the device takes these actions only in response to the user's command. Find My iPhone includes Activation Lock, which is designed to prevent anyone from turning off Find My iPhone, erasing a device or reactivating it. (107)
- BlackBerry Protect is an integrated, OS-based solution that provides tamper-resistant theft prevention to BlackBerry 10 devices by disabling all non-essential device functionality when theft is detected (essential functionality includes recovery screen and emergency calls to 911). Theft-mode is triggered when the device holder fails the password authentication ten times or when the registered owner with BlackBerry ID credentials remotely reports the device stolen via the BlackBerry Protect website. (108)
- Microsoft provides Find My Phone as a free service on all Windows Phone OS-based smartphones. To use the feature, users sign in to a secure web portal using their Microsoft account credentials tied to the smartphone; once authenticated, users can request the smartphone's current location, cause it to ring, lock it and leave a custom message, or erase user data on it to protect personal information. (112)
- Motorola Mobility's Moto Care service allows users to remotely lock, wipe, locate and ring the device from a web portal. (113)
- Qualcomm with Qualcomm® SafeSwitch™ technology, SafeSwitch-enabled devices can be remotely locked at a very deep level if they are lost or stolen. SafeSwitch commands are processed and authenticated by hardware, making potential attacks, such as malicious locking of phones and unlocking stolen phones, far less feasible. SafeSwitch™ works in full harmony with Lookout Mobile Security, and can be integrated to other solutions as requested by the operator. (115)

[5] *See,* Report Recommendation 1.3 at p. 69.

- Samsung - Samsung solution is comprised of two parts “Reactivation Lock” and “Find My Mobile”. “Reactivation Lock” is designed to prevent access to the device after it has been lost or stolen. It uses Samsung account to regain access and use of the device. Samsung account authenticates and authorizes protection of your personal information. “Find My Mobile” allows the user to manage their device by locating, locking, wiping, unlocking and receiving SIM change alerts. Both of these solutions are described in the following subsections. (116)
- Third party solutions also have a major role. – (LoJack 118)
- Android – “Android Device Manager”. Non-Technical Description, Capabilities & Functions • Current release version (Android 2.2 and newer) allows user to remotely locate, lock, and erase an Android phone or tablet from the Device Manager App or web interface over a wireless Internet data connection.

III. Support Voluntary Database Solutions

The Carrier-CTIA voluntary consumer initiative, as outlined in the Report, deserves commendation. In light of carrier relationships with their customers, the likely first step for a consumer with a lost or stolen phone is to contact their mobile operator. The steps outlined in the industry initiative significantly ease the potential burden on consumers. This approach uses a strategy of making stolen phones effectively less “non-transferable,” thereby significantly reducing the incentives for stolen phone by eliminating the market for them.

While encouraging consumers to record their device ID numbers is certainly laudable, a streamlined process might include retaining the information at the time of activation. Even consumers who actually do retain their device ID information may not have it readily accessible when reporting a missing phone.

IV Role of Device Identifiers

The Report appropriately highlights the contribution that unique device identifiers make to technology. Although operating in the background, these identifiers perform a variety of functions critical to device functionality. As discussed in detail in the report, these identifies are also critical to creating actionable information to carriers.

In the future, TIA anticipates that many additional contributions can be made by unique device identifiers in the future to enhance public safety and health. For example, remote sensing devices can communicate timely information to the appropriate action. Unique identifiers in these contexts will be an important component of an interactive process for M2M communications. Some of these potential applications are likely to be outside of commercial radio services.

The numbering space for these devices spans many types of identifiers and include services generally outside the Commission's purview. Consequently these device identifiers should continue to remain with industry. TIA cautions against any initiatives that might restrict or impede device manufacturers from obtaining identifiers. Device security should not impact the conservation of the numbering space resources with any restrictive approaches.

Regarding TAC recommendations 1.4, 1.5, 1.6,[6] TIA encourages the consultation process to include all stakeholders involved in device numbering, including TIA as the Global Hexadecimal

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

Administrator. MEID Administrator for Global Hexadecimal and RR99 multimode Decimal identifiers. TIA is an ideal candidate for increasing security of mobile network identifiers both from a Standards Development Organization perspective and as MEID Administrator for Global Hexadecimal including RR99 multimode Decimal identifiers.

The concern expressed in the report about "counterfeiters can impersonate legitimate smartphones" deserves to be underscored. The success of the other database initiatives to identify stolen smart phone depends appropriate measures to counteract counterfeiting.

---

investigation. Recommendation 1.5: The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.
Recommendation 1.6: The FCC TAC recommends that CTIA convene a joint Law Enforcement, carrier, and wireless industry task force to define a consumer outreach process to encourage consumers to initially report smartphone thefts to their carrier.

V. CONCLUSION

TIA strongly supports the Commission's goal to using technology based tools to assist both consumers and law enforcement to reduce mobile phone theft.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

January 30, 2015