



**Testimony of  
Gerry Keegan  
CTIA-The Wireless Association  
In Opposition to Senate Bill 310**

**March 3, 2016**

**Before the Connecticut General Assembly General Law Committee**

Co-Chairs Leone and Baram and members of the Committee, I am Gerry Keegan with CTIA, the trade association for the wireless communications industry, in opposition to Senate Bill 310. Because the wireless industry has fulfilled its commitment to provide anti-theft functionalities on smartphones, this bill is unnecessary.

In July 2015, the U.S. wireless industry announced that it fulfilled its commitment to provide anti-theft (aka "kill switch") functionalities that give U.S. consumers – at no cost – new protections in the event their smartphones are lost or stolen.<sup>1</sup> These anti-theft functionalities include capabilities to remotely lock and wipe missing devices, render the smartphone inoperable to an unauthorized user, prevent reactivation without the authorized user's permission (including unauthorized factory reset attempts) to the extent technologically feasible, reverse the inoperability if the smartphone is recovered by the authorized user, and restore user data on the smartphone to the extent feasible. As part of this commitment, these functionalities are pre-loaded on devices or downloadable.<sup>2</sup>

---

<sup>1</sup> See Wireless Industry Delivers on Smartphone Anti-Theft Voluntary Commitment, available at: <http://www.ctia.org/resource-library/press-releases/archive/wireless-industry-delivers-on-smartphone-anti-theft-voluntary-commitment> (last visited Feb 29, 2016).

<sup>2</sup> See Smartphone Anti-Theft Voluntary Commitment, available at: <http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment> (last visited Feb 29, 2016).



Additionally, the wireless industry announced a new effort in October 2015 to encourage the widespread adoption of these anti-theft functionalities by consumers.<sup>3</sup>

The wireless industry's fulfillment of its commitment to provide consumers with "kill switch" functionalities on smartphones, which has strengthened the fight against smartphone theft, negates any need for legislation on this issue. In fact, Consumer Reports noted in June 2015 that smartphone thefts have dramatically declined, while law enforcement in major U.S. cities also reported significant declines that they attributed to the use of these anti-theft functionalities.<sup>4</sup>

In addition to the deployment of "kill switch" technology, the wireless industry has undertaken a number of steps to assist law enforcement in their efforts to address smartphone theft. Most recently, CTIA released a proposal in February 2016 to develop a central portal to report lost and stolen mobile devices. Using multiple source databases, the mobile device information portal will provide timely, succinct responses so that consumers and commercial resellers know if a mobile device is reported lost or stolen before they purchase it.<sup>5</sup> In addition, law enforcement will be able to check and, hopefully, return found mobile devices to their authorized users. Federal Communications

---

<sup>3</sup> See CTIA and Participating Wireless Companies Announce New Effort to Help Consumers Combat Stolen Smartphones and Protect Personal Information, *available at*: <http://www.ctia.org/resource-library/press-releases/archive/ctia-announce-update-stolen-phone-agreement> (last visited Feb 29, 2016).

<sup>4</sup> Calla Deitrick, *Smartphone thefts drop as kill switch usage grows*, Consumer Reports (June 11, 2015), <http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm>.

<sup>5</sup> See Mobile Device Theft Prevention Industry Initiative Announces Request for Proposal for Mobile Device Information Portal, *available at*: <http://www.ctia.org/resource-library/press-releases/archive/mobile-device-theft-prevention-industry-initiative-announces-request-for-proposal-for-mobile-device-information-portal> (last visited Feb 29, 2016).



Commission (FCC) Chairman Tom Wheeler lauded this most recent announcement noting that law enforcement and consumers need tools like this portal.<sup>6</sup>

In November 2013, national wireless carriers announced the deployment of an internationally integrated stolen phones database.<sup>7</sup> These carriers use the database to check whether a smartphone presented to them has been reported stolen. If the smartphone has been reported stolen, it will be denied service on carrier networks. The database is interconnected across mobile carriers and is a resource for law enforcement to use to deter thefts. In collaboration with carriers, local law enforcement should make extensive use of the industry's stolen phones database and corresponding solutions. I would like to take this opportunity to invite Connecticut law enforcement agencies to seek access to the database. This stolen phones database will be one source for the recently announced mobile device information portal.

The wireless industry has also been individually and collectively educating consumers on ways to help reduce smartphone theft. These initiatives include highlighting consumer use of passwords and pins, applications, and other preventative measures so that if a consumer's smartphone is ever lost or stolen, personal information is protected. These education efforts include information at the time of smartphone

---

<sup>6</sup> Wheeler, T. [TomWheelerFCC]. (2016, February 8). Consumers, law enforcement need tools like the new portal by @CTIA to combat cell phone theft. <http://bit.ly/1TOcxmG> [Tweet]. Retrieved from <https://twitter.com/tomwheelerfcc?lang=en>.

<sup>7</sup> See CTIA Announces Wireless Providers Completed Final Deadline to Create a Database for Stolen 4G/LTE Devices, available at: <http://www.ctia.org/resource-library/press-releases/archive/ctia-announces-wireless-providers-completed-final-deadline-to-create-a-database-for-stolen-4g-lte-devices> (last visited Feb 29, 2016).



activation and through public service announcements, websites, e-mail, and social media outreach.

The wireless industry remains committed to working with all stakeholders to help combat smartphone thefts. We are, for example, active participants in the FCC's Mobile Device Theft Prevention Working Group. This group regularly meets to address five key areas on this issue, including problem definition, existing and advanced solutions, gap analysis, cybersecurity and privacy, and law enforcement and consumer outreach.

In closing, the wireless industry has been at the forefront of addressing smartphone thefts. The industry's ongoing multi-layered efforts eliminate the need for new legislation on this issue. For these reasons, we respectfully ask that you not move SB 310. Thank you for your consideration.

## Wireless Industry Delivers on Smartphone Anti-Theft Voluntary Commitment

**WASHINGTON**, July 1, 2015 – Today, CTIA-The Wireless Association® announced the wireless industry's fulfillment of the Smartphone Anti-Theft Voluntary Commitment that gives U.S. consumers – at no cost – new protections in the event their smartphones are lost or stolen. Included are capabilities to remotely lock and wipe missing devices while still enabling 9-1-1 calls even when the phone is locked and providing the consumer a means to unlock the phone when it is recovered. The industry will also maintain its proactive consumer education and outreach campaign to deter theft. Participating companies are Apple Inc.; Assurant, Inc.; Asurion; AT&T; BlackBerry Limited; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics MobileComm USA, Inc; Motorola Mobility LLC; Microsoft Corporation; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon Wireless; and ZTE USA, Inc.

Please attribute the following statement to CTIA President and CEO Meredith Attwell Baker:

"Today's fulfillment of the Smartphone Anti-Theft Voluntary Commitment is another example of the wireless industry proactively working together with policymakers and law enforcement to help protect consumers' smartphones in the event they are ever lost or stolen. As media reports indicated from San Francisco to New York City, these efforts are significantly reducing device thefts across the country. We will continue to work with all interested parties to continue to deploy new technologies and tools to improve device theft deterrence tools. We remind consumers to take a few minutes to use PINs, passwords, apps and other device features – many of which we list on our website – to protect their mobile devices and personal information."

###

*CTIA-The Wireless Association® ([www.ctia.org](http://www.ctia.org)) represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices and initiatives and convenes the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.*

*Twitter: [@ctia](https://twitter.com/ctia) | Blog: <http://ctia.it/Na6erv> | Facebook: <http://ctia.it/LCm4Nn> |  
LinkedIn Group: <http://ctia.it/Na6cA2> | Google+: <http://ctia.it/12PfCrO>*

**Press Contact:** Amy Storey, [astorey@ctia.org](mailto:astorey@ctia.org), 202-736-3207



## Smartphone Anti-Theft Voluntary Commitment

### Part I

Each device manufacturer and operating system signatory of Part I of this "Smartphone Anti-Theft Voluntary Commitment" agrees that:

A. 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 that provides the connected capability to:

1. Remote wipe the authorized user's data (i.e., erase personal info that is added after purchase such as contacts, photos, emails, etc.) that is on the 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 911 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., "phone home").
3. Prevent reactivation without 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).

B. In order to be effective, the anti-theft tools need to be widely adopted while still respecting the importance of consumer choices and privacy. New models of smartphones first manufactured after July 2016 for retail sale in the United States will, if technically necessary, make readily available to the authorized user an option that allows the authorized user to enable or disable the anti-theft solution at any time that the smartphone is connected and is in the authorized user's possession.

In addition to this baseline anti-theft tool, consumers may use other technological solutions, if available for their smartphones.

### Part II

Each network operator signatory of Part II to the "Smartphone Anti-Theft Voluntary Commitment" commits to permit the availability and full usability of a baseline anti-theft tool to be preloaded or downloadable on smartphones as specified in this commitment.

###

The following network operators, device manufacturers and operating system companies are participating in the voluntary commitment: Apple Inc.; Assurant; Asurion; AT&T; BlackBerry; Google Inc.; HTC America Inc.; Huawei Device USA, Inc.; LGE Mobile Research U. S. A., LLC; Microsoft Corporation; Motorola Mobility LLC; Samsung Electronics America, Inc.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon and ZTE USA Inc.

For more information, please visit the [Smartphone Anti-Theft FAQ](#).

*Last Updated: October 2015*

