



January 30, 2015

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

**Re: December 4, 2014 Letter - FCC Technological Advisory Council
Subcommittee Report on Mobile Device Theft Prevention;
FCC ET Docket No. 14-143**

Dear Chairman Wheeler:

I am writing on behalf of T-Mobile USA, Inc.¹ in response to your December 4 letter to John Legere regarding the report by the FCC's Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention. We agree that smartphone theft is an important problem facing consumers and with the report's finding that there is no single technology solution that will eliminate phone theft (*i.e.*, no "silver bullet"); as such, a complementary suite of technical and operational mitigation techniques will be needed to address the problem.

T-Mobile has been actively working with other stakeholders in the wireless ecosystem in identifying a variety of solutions to help mitigate handset theft. To this end, all iOS and Android smartphones sold by T-Mobile include security software that allows subscribers to remotely locate, lock and wipe personal data from stolen handsets. T-Mobile also actively participates in industry-wide programs to deter handset theft. We joined other wireless carriers, handset manufacturers and CTIA in working with the Federal Communications Commission and Major City Police Chiefs to develop a program to deter handset theft, culminating in the April 2012 Voluntary Commitment between the FCC and members of CTIA. Pursuant to that Voluntary Commitment, in October 2012, T-Mobile established connectivity with the GSMA Global IMEI Database, where stolen devices are listed in a comprehensive database to help prevent their use on another carrier's GSM/LTE network.

T-Mobile is also working with Operating System vendors and handset manufacturers so that smartphones manufactured after July 1, 2015 will include additional anti-theft functionality. This technology will have the capability to render the essential features of a stolen smartphone inoperable and to withstand a hard reset to the handset's original factory settings. It will also allow an authorized user to restore the functionality of a stolen phone upon recovery.

T-Mobile supports industry-wide efforts to reduce the impact of mobile handset theft and we look forward to continuing to work with the FCC through the TAC and other groups on this important initiative. With respect to the three specific recommendations in your letter, T-Mobile has already implemented them or is taking steps to begin implementation, as follows:

- **Lock, Wipe, Restore:** As discussed above, iOS and Android smartphones sold by T-Mobile contain software that allows subscribers to remotely locate, lock and wipe personal data from stolen handsets – either preloaded or available for download. Microsoft has introduced technology that allows an authorized user to remotely lock, wipe data from and reset the passcode on a stolen Windows handset. The Windows solution will be available to T-Mobile subscribers

¹ T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded corporation that is incorporated in the State of Delaware.



in 2015. By “restore” we understand you are referring to the ability of a consumer to restore essential features of a recovered handset that were rendered inoperable by a “kill switch.” This feature is currently available for iOS smartphones sold by T-Mobile and, as required by the recently-enacted California statute, we have informed our handset manufacturers that smartphones sold by T-Mobile that are manufactured on or after July 1, 2015 must include that feature.

- **IMEI:** The IMEI is fixed by the manufacturers during the process of manufacturing handsets. While T-Mobile does not manufacture mobile handsets, we will continue to include in our handset specifications a requirement that the IMEI must be unchangeable on each device T-Mobile purchases. If the IMEI is tampered with, the handset is required to display an error message informing the user that the phone has been flashed with unauthorized software and is locked. Not only does this “no-tampering” requirement deter handset theft, but it also allows T-Mobile to use the unique IMEI for other essential purposes, including billing, customer care, third-party billing, and application use/functionality. In addition, we have joined others in the wireless industry in supporting federal legislation that seeks to criminalize IMEI tampering, such as the legislation introduced by Senator Schumer of New York.
- **Availability of Data Regarding Stolen Handsets:** T-Mobile currently uploads information regarding lost or stolen phones to the GSMA IMEI Database “blacklist” on a daily basis. We understand the benefits of more frequent dissemination of data to this Database, but recognize the challenges in finding an efficient solution. We believe that GSMA is committed to work with the US wireless operators to move as nearly as possible to the real-time exchange of data between the wireless operators and the GSMA Global IMEI Database.

Finally, you have asked about steps T-Mobile takes to ensure that stolen devices are not activated for service on T-Mobile’s network. Whenever a used device is brought by a customer into a T-Mobile retail store, during the activation process the retail representative enters the IMEI of the device into T-Mobile’s computer system where it is automatically checked against an industry-wide database to ensure that it has not been reported as lost or stolen. If the handset appears on the database as stolen, it will not be activated. T-Mobile also maintains an “IMEI Checker” on its public website (<http://www.t-mobile.com/verifyIMEI.aspx>), which allows consumers to check whether a particular device has been reported as lost or stolen.

Thank you again for your letter and for giving us the opportunity to respond to your inquiry. Please feel free to contact me if you have additional questions for T-Mobile.

Sincerely,

A handwritten signature in black ink that reads 'Andy Levin'.

Andy Levin
Senior Vice President, Government Affairs

cc: Maria Kirby
Deborah Ridley
Charles Mathias