This document is made available electronically by the Minnesota Legislative Reference Library as part of an ongoing digital archiving project. http://www.leg.state.mn.us/lrl/lrl.asp

Excerpt from MN Statute:

ARTICLE 1

SMART PHONE ANTITHEFT PROTECTION

Section 1. **[325F.698] SMART PHONE ANTITHEFT PROTECTION.**

Subdivision 1. **Definitions.** (a) For the purposes of this section, the following terms have the meanings given them. (b) "Smart phone" means a cellular phone or other mobile device that: (1) is built on a smart phone mobile operating system; (2) possesses advanced computing capability; (3) enables network connectivity; and (4) is capable of operating on a long-term evolution network and successor wireless data network communication standards. Capabilities a smartphone may possess include, but are not limited to, built-in applications, Internet access, digital voice service, text messaging, e-mail, and Web browsing. Smart phone does not include a phone commonly referred to as a feature or messaging phone, a laptop computer, a tablet device, or a device that has only electronic reading capability.

Subd. 2. **Antitheft functionality required.** Any new smart phone manufactured on or after July 1, 2015, sold or purchased in Minnesota must be equipped with preloaded antitheft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost.

EFFECTIVE DATE. This section is effective July 1, 2015.

Sec. 2. **REPORT ON SMART PHONE ANTITHEFT FUNCTIONALITY.**

Wireless telecommunications equipment manufacturers, operating systems providers, and wireless telecommunications service providers must either individually or jointly, by January 15, 2015, submit a report to the chairs and ranking minority members of the legislative committees with primary jurisdiction over telecommunication issues. The report must describe the principle functions of a baseline antitheft tool that manufacturers and operating system providers will utilize on new models of smart phones in order to comply with section 1, and must describe the technology or functions included to ensure the baseline antitheft tool is easily operable by individuals with disabilities.

Title: JOINT REPORT ON SMARTPHONE ANTITHEFT FUNCTIONALITY

1. Executive Summary

In accordance with Section 2 of 325F.698, SMART PHONE ANTITHEFT PROTECTION, the wireless telecommunications equipment manufacturers, operating systems providers, and wireless telecommunications service providers must individually or jointly submit a report to the chairs and ranking minority members of the legislative committees with primary jurisdiction over telecommunication issues. The report must describe the principle functions of a baseline antitheft tool that manufacturers and operating system providers will utilize on new models of smart phones in order to comply with section 1, and must describe the technology or functions included to ensure the baseline antitheft tool is easily operable by individuals with disabilities. The joint report contained herein complies with the reporting requirement as outlined in Section 2.

2. Introduction

Any new smartphone manufactured on or after July 1, 2015 sold or purchased in Minnesota must be equipped with preloaded anti-theft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost. The joint report herein describes the baseline anti-theft tool that complies with 325F.698 for manufacturers, operating system providers and wireless service providers.

3. Overview & Scope

In response to Section 2 of 325F.698, SMART PHONE ANTITHEFT PROTECTION, the following constitutes the REPORT ON SMART PHONE ANTITHEFT FUNCTIONALITY. Wireless telecommunications equipment manufacturers, operating systems providers, and wireless telecommunications service providers jointly submit the report herein to the chairs and ranking minority members of the legislative committees with primary jurisdiction over telecommunication issues. The scope of this report describes the principle functions of the baseline antitheft tool that manufacturers and operating system providers utilize on new models of smart phones in order to comply with section 1, and describes the technology or functions included to ensure the baseline antitheft tool is easily operable by individuals with disabilities.

4. Description of Baseline Anti-Theft Tool

On April 15 of 2014, CTIA and participating companies announced the Smartphone Anti-Theft Voluntary Commitment (“Commitment”) which is the most recent effort by the industry to help aid law enforcement to deter smartphone thefts in the United States. The industry has committed

to providing this tool to consumers and to law enforcement, which will further strengthen the fight against smartphone theft. It reads as follows:

> Part I - Manufacturers and Operating System Providers
>
> Smartphone manufacturers and operating system providers listed in the Appendix offer, for new models of smartphones first manufactured after July 2015 for retail sale in the United States, 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).
>
> In addition to this baseline anti-theft tool, consumers may use other technological solutions, if available for their smartphones.
>
> Part II - Wireless Telecommunications Service Providers
>
> ***Each wireless telecommunications service provider listed in the Appendix commits to permit the availability and full usability of a baseline anti-theft tool to be preloaded or downloadable on smartphones as specified in Part I.***

Device Solutions

This section describes the following existing device solutions for the prevention of the mobile device theft (this section lists manufacturers and operating system providers, as carriers have agreed to Part II of the Commitment). It should be noted the progress report listed below does not illustrate all that the manufacturers have done and that some manufacturers rely on and are working with the Operating System providers on solutions:

- Apple
- BlackBerry
- Google
- LG
- Microsoft
- Motorola
- Qualcomm
- Samsung

The descriptions for each of the device solutions which cover the following topics:

- Non-Technical Description, Capabilities & Functions
- Level of Accessibility and Funding Model
- Status of Availability
- Reference URL

Apple

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.

Non-Technical Description, Capabilities & Functions

- Find My iPhone allows for users to remotely locate their device, play a sound on it, or erase it, all in a privacy friendly manner where the device only connects to the Find My iPhone service on prompting from a user, giving the user complete control over it.
- With iOS 7, Apple introduced Activation Lock, whereby a phone enrolled in Find My iPhone cannot be reactivated following an erase/reset without the user entering their iCloud username and password. This makes Activation Lock a reversible solution that enables users to restore their device if they recover it.
- For devices that support Apple Pay, users can suspend Apple Pay by placing their device in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone. When a user erases a device using Find My iPhone, the cards on the device are placed into an unusable state.

Level of Accessibility and Funding Model

- Find My iPhone works on any iOS device running iOS 5 or above. Activation Lock is supported on devices running iOS 7 and above. Find My iPhone is available to iOS users for free at no extra cost.

Status of Availability

- Available now.

Reference URL

- https://www.apple.com/icloud/find-my-iphone.html.

BlackBerry

BlackBerry Protect is an integrated, OS-based solution that provides tamper-resistant theft prevention to BlackBerry 10 devices by disabling all 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. Theft-mode triggering also automatically executes a complete device data wipe so that all consumer information is further protected (in addition to data encryption). The BlackBerry Protect website also allows registered owners to find their lost devices via location services. Recovered devices may have theft-mode deactivated either directly through the user interface recovery screen with the registered owner's BlackBerry ID credentials or via a secure "reverse logistics" field utility that supports authorized parties in service and support environments.

Non-Technical Description, Capabilities & Functions

- Device-based solution that leverages BlackBerry ID consumer credentials so that registered owners can report stolen devices, thereby blocking all functionality of devices except for device recovery screen and emergency calls. Theft-mode can also be triggered automatically on the device when the device holder fails the required password authentication for device start-up or log-on.
- BlackBerry Protect also provides other consumer remote security functionality, including locating devices via GPS and device data wiping.

Level of Accessibility and Funding Model

- BlackBerry Protect with theft prevention service included with device purchase.

Status of Availability

- Available in accordance with MN law.

Reference URL

- Not currently available.

Google

The current in-market solution available from Google is called "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. Below is a subset of the current features:
  - Users can remotely ring devices at maximum volume so user can find it (even if it's been silenced)
  - Users can remotely reset the device password.
  - Users can remotely factory reset the device.
  - Users can locate the device on graphical map in real time.
  - Users can add a dial-back number on the locked device, so that they can be reached if a lost phone is found.
  - Users can connect as many compatible Android devices as desired to Android Device Manager.
  - Administrators and users can remotely wipe a lost or stolen device through the Google Apps Admin Console, for mobile devices that are synced to that organization's Google Apps account (applicable to Google Apps for Work, Education, Nonprofits, etc.)
- Note: In addition, Android Device Manager devices running Android 4.4 or earlier also have device encryption available as an option and it is enabled by default in Android 5.0. By default, encrypted Android devices require a user to enter a PIN or password that is required whenever the device is booted up or attempted to be wiped.

Status of Availability

- In-Market.

Reference URL

- https://support.google.com/accounts/answer/3265955?hl=en.
- https://support.google.com/nexus/answer/4596836?hl=en-GB.

- https://support.google.com/accounts/answer/3265955?hl=en.
- http://googleblog.blogspot.com/2013/08/dude-wheres-my-phone-simple-steps-to.html.
- https://support.google.com/a/answer/173390?hl=en Google Apps.

Administrators and users can remotely wipe a lost or stolen device through the Google Apps Admin Console, for mobile devices that are synced to that organization's Google Apps account (applicable to Google Apps for Work, Education, Nonprofits, etc.).

LG

The solution available from LG is called "LG Anti-Theft Solution" and uses McAfee. It is based on Android OS and can be remotely operated to impose restrictions or trigger functions to protect data through wiping out, backing up and restoring, drawing attention, or determining the current location of the smartphone as long as there is internet connectivity, via a cellular network or Wi-Fi. In addition, manipulation of the smartphone through factory-reset and USB connections are also blocked when the device is remotely locked. Key characteristics and descriptions of the solution are summarized as:

Non-Technical Description, Capabilities & Functions

- User can locate and track the device, lock it or wipe the data out using the service website.
- User can backup and restore data using the application and the web service.
- Factory-reset and USB connection are also blocked when the device is remotely locked.

Level of Accessibility and Funding Model

- Available on all Android smart phones shipping after July 1, 2015. No fee for end users (customers).

Status of Availability

- In-market Q1 2015 timeframe.
- Upgrades to substantial subset of existing devices possible (TBD).

Reference URL

- http://lge.mcafeemobilesecurity.com.

Microsoft

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. Network connectivity—cellular, cellular data, or Wi-Fi—is required to deliver commands to the smartphone. A unique, secure, proprietary hardware identifier is used to link a smartphone to an account and target commands to it.

By July 2015, new features in the Windows Phone OS will offer additional functionality to prevent an unauthorized user from using the smartphone after resetting or reflashing the operating system to further reduce the value of a stolen Windows Phone. These changes will meet Microsoft's commitment to the CTIA Smartphone Anti-Theft Voluntary Commitment and in accordance with MN law.

Non-Technical Description, Capabilities & Functions

- Built-in to every Windows Phone, Find My Phone provides remote Locate, Ring, Lock, Message, and Erase capabilities.
- Locate and Ring help find and discover a lost or stolen device.
- Lock prevents access to customer information on the device until it can be recovered or reset.
- Message is an optional part of Lock to display a message on the screen (e.g., a number to call or address to email).
- Erase reformats user information to protect privacy of personal data.
- As long as there is connectivity, users are always able to perform a remote action – there is no on/off switch for the existing Find My Phone features, but users must expressly request an action by logging into a website with their Microsoft account.
- Users can choose to periodically report device location automatically so a last known location is always available even if the device is powered off.

Level of Accessibility and Funding Model

- Built into every Windows Phone device since October 21, 2010.
- Available to all users for free as long as they connect a free Microsoft Account to the device.

Status of Availability

- Actively maintained and developed by Microsoft.
- Most recent software update shipped to customers in May 2014 as part of Windows Phone 8.1.

- Ongoing backend and website updates ship regularly without requiring any user action.
- Publicly committed to support CTIA commitment with additional functionality offered at no fee to end users to prevent an unauthorized user from using the smartphone after resetting or reflashing the operating system for Windows Phone smartphones manufactured after July 1, 2015.

Reference URL

- Find My Phone for users (*login required*): http://www.windowsphone.com/find.
- Find My Phone support info: http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/find-a-lost-phone.

Motorola

The solution available from Motorola is called "Lost Phone Web Portal/Moto Care". In addition, Motorola implements Google's Android Device Manager solution for remote lock/wipe.

Non-Technical Description, Capabilities & Functions

- Currently release version allows user to lock device screen on device UI, or remotely with internet connectivity.
  - Can post a message on screen.
- User can remotely ring device at maximum volume so user can find it (even if it's been silenced).
- User can locate device on graphical map, in real time.
- User can quickly and securely erase all User data on the device.

Level of Accessibility and Funding Model

- Currently free to customer.

Status of Availability

- In-Market with devices Moto X, G, E, Droid Ultra, Droid Maxx.

Reference URL

- https://motorola-global-portal.custhelp.com/app/answers/detail/a_id/95507.

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.

Non-Technical Description, Capabilities & Functions

- Users can locate, track, wipe, ring, message, or lock their devices using the service portal.
- When locked, devices can mitigate a very wide range of both physical and software based attempts to defeat the lock mechanism.
- Bypassing or defeating the software and OS will not enable malicious locking or unlocking of the device at a hardware level.
- Reversing the lock on a device may be done locally on the device or remotely. It is only possible by using credentials provided with a session-specific unlock key from the SafeSwitch™ service portal.

Level of Accessibility and Funding Model

- Available to OEMs on chipsets starting Q2'2015.

Status of Availability

- Chipsets available at the beginning of Q2'2015.

Reference URL

- https://www.qualcomm.com/products/snapdragon/security.

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 remotely manage their device via website by locating, locking, unlocking, wiping the smart phone and receiving SIM change alerts. Both of these solutions are described in the following subsections.

Samsung Reactivation Lock

Non-Technical Description, Capabilities & Functions

- Reactivation Lock prevents device from reactivation after a factory reset.

- When Reactivation Lock is engaged the device will be locked and prevents access beyond the device setup screens.
- Consumer credentials (Samsung account name and password) are required to be entered bypass Reactivation Lock.
- Must be activated by the consumer before functionality is available.

Level of Accessibility and Funding Model

- Provided at no cost to consumer on technically capable devices.

Status of Availability

- Some models of Galaxy Note 3.
- Most models of Galaxy S5.
- Additional models to be added for compliance with state laws.

Reference URL

- What is Reactivation Lock and how do I use it? http://www.samsung.com/us/support/howtoguide/N0000002/17296/229710/SCH-N330PWLXAR

Samsung Find My Mobile Solution

Non-Technical Description, Capabilities & Functions

- Web based solution which allows the consumer to remotely **control** their device.
- Features include the ability to locate, lock/unlock, retrieve call logs, wipe device, get alerts if SIM-card has changed, ring device and enable emergency mode.

Level of Accessibility and Funding Model

- No fees to use this service.

Status of Availability

- In market since 2011, launched in 181 countries in over 40 languages.

Reference URL

- http://findmymobile.samsung.com.

- **Wireless Service Providers are currently in compliance with Part II of the Commitment.**

- **Description of Functions operable by individuals with disabilities**

  Mobile device operating systems by default provide methods for individuals with disabilities to operate a mobile device. These methods allow persons with limitations in vision, hearing, dexterity or learning to effectively operate the device and the anti-theft features. As the systems are continually improving, we recommend the chairs and ranking minority members review the details of the specific accessibility features from the below sources.

  - Android-http://developer.android.com/design/patterns/accessibility.html
  - iOS-http://www.apple.com/accessibility/ios/
  - Windows Phone 8-http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/accessibility-on-my-phone
  - The Mobile Manufacturers Forum[1]–http://www.gari.info

5. Summary Comments

The wireless industry has a history of working with stakeholders to provide tools to consumers and law enforcement to combat the theft of smartphones. In April of 2012, we announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data. As a part of that commitment, in November 2013, wireless carriers completed a stolen phones database to report and track all stolen 4G/LTE phones in the U.S. The stolen phones database enables devices to be de-activated and re-activated if necessary. Wireless carriers use the database to check whether a device presented to them has been reported lost or stolen. If a device has been reported lost or stolen, it will be denied service on carrier networks.

In addition to the deployment of the integrated database, the wireless industry has been individually and collectively educating consumers on ways to help reduce smartphone theft. These initiatives include highlighting consumer use of passwords, applications, and other preventative measures so that if the consumers' smartphones are ever lost or stolen, their personal information is protected. These education efforts include information at the time of smartphone activation, public service announcements, websites, e-mail, and social media outreach.

[1] Run by the Mobile Manufacturer's Forum, the Global Accessibility Reporting Initiative is a project designed to help consumers learn more about the accessibility features of mobile devices and to help them identify devices with the features that may assist them with their particular needs.

As noted above, on April 15 of 2014, CTIA and participating companies announced the Smartphone Anti-Theft Voluntary Commitment ("Commitment") which is the most recent voluntary effort by the industry to help aid law enforcement to deter smartphone thefts in the United States. Specifically, this commitment states 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 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).

The industry was also very involved in the FCC's Technological Advisory Committee's ("TAC") recommendations coming out of the Mobile Device Theft Prevention ("MDTP") Working Group[1]. FCC Chairman Wheeler directed the TAC in June to form a working group to develop industry-wide recommendations to mitigate "the increasing theft of mobile devices, which has become a major source of crime in the United States." This Working Group is comprised of representatives from key industries involved in mobile technologies, members of law enforcement and consumer interest groups, and includes representatives from CTIA and member companies. The MDTP Working Group issued its recommendations to Chairman Wheeler on December 4th. The FCC has now asked for public comment on the report.

This report shows that much progress has been made by the wireless industry in providing tools to consumers that can be used in the event that their smartphone is lost or stolen. Many companies have already made baseline anti-theft tools available to consumers, with others having made substantial progress. This is being done in accordance with the "Smartphone Anti-Theft Voluntary Commitment", as well as Minnesota law. Additionally, these anti-theft tools are being provided to consumers at no additional cost, in line with the "Commitment" and Minnesota law.

Appendix: List of Equipment manufacturers, operating systems providers, and wireless telecommunications service providers participating in this report

[1] http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf

Current List:

Apple Inc.; Asurion; AT&T; Cricket Wireless LLC; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics Mobile Research LLC; Motorola Mobility LLC; Microsoft Corporation; Nokia, Inc.; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon Wireless and ZTE USA Inc.