

Smart Device Theft Prevention (SDTP)



Presented by:

Celeste L. McCray
Consumer Education and Outreach Specialist
Consumer and Governmental Affairs Bureau
(CGB)
Federal Communications Commission (FCC)

Background Statistics:

- In 2013, 3.1 million Americans were victims of mobile device theft, and 1.4 million Americans simply loss their mobile device (Consumer Reports).
- 113 cell phones are lost or stolen every single minute in the United States. In a 24 hour period, Americans have lost seven million dollars (\$7M) in expensive mobile devices. (plateautel.com)
- 40%-69% of theft in major cities (Washington, DC, New York, San Francisco) around the country involves mobile devices. Losing your mobile devices can cause a wide range of personal and professional hardships.

Background/Statistics (cont.):

- 50% of mobile device victims are willing to pay up to \$500.00 to retrieve their stolen equipment. (IDG Research)
- More than half (54%) choose to not install anti-theft apps when they discover how much personal data was being obtained. (Pew Internet.org)
- 30% of app users have uninstalled apps that was already pre-loaded on their mobile device when it found that the app was collecting personal data that they didn't want to share. (Pew Internet.org)

Privacy Issues:

- 12% of mobile device users had someone access their information that made them feel as if their privacy was invaded.
- 14% of teens posted their home address online. (McAfee)
 - This personal information becomes a footprint on social networking sites.
 - It is also important to note that we use our mobile devices to shop online, access banking information and update social media websites.
 - This information can be stored on mobile devices and can potentially be a used to compromise privacy.

FCC's Role Technical Advisory Council

In 2014, FCC's Chairman Tom Wheeler requested the creation of a Technical Advisory Committee (TAC) which would serve as a working group on "Mobile Device Theft Prevention" (MDTP).

Currently, industry groups have developed voluntary commitments and best practices on deterring mobile theft and asked their members to adopt them.

It is important that the FCC provide national leadership in this area.

FCC Role (Cont. p.2)

The mission of the MDTP TAC working group is to explore problems of mobile device theft and develop industry-wide recommendation.

The Commission's working group has established five (5) subgroups to focus on finding solutions to mobile device theft.

The subgroups are:

- Problem Definition
- Existing Solutions
- Gap Analysis
- Cyber security & Privacy
- Consumer Outreach

CGB's Role and Outreach Efforts:

CONSUMER OUTREACH EFFORTS:

CAOD Webpage:

Developed a section of our CAOD webpage is dedicated to mobile device theft prevention.

www.fcc.gov/outreach

Outreach Toolkit:

Created Consumer Guides, Blogs, Flyers, Talking Points, and helpful links to wireless carrier numbers on stolen mobile devices.

- An example of toolkit designed for our law enforcement community can be found at: <http://www.fcc.gov/guides/smart-device-protection-toolkit-law-enforcement>

FCC Call Center

Established messaging with our national call center.

Consumer Outreach Efforts (Cont. p.3)

Partner with Key Stakeholders

- Consumer Advocacy Organizations
- Wireless Carriers
- Law Enforcement Agencies
- Schools
- Libraries
- Other Federal and State Government Agencies)

Conduct Public Education and Community Outreach Events:

- Just like the webinar today (Tuesday, March 31, 2015)

Best Practices: Prior to Mobile Device Theft

Steps to take prior to mobile device theft are:

- Always lock your phone with:
 - a pin number (do not share this pin number)
 - finger print
 - face recognition software.
- Always back up data
 - On a computer
 - In the cloud
- Always record your unique mobile device identifier in a safe place.
 - MEID (Mobile Equipment Identification)
 - IMEI (International Mobile Equipment Identifier)
 - ESN (Electronic Serial Number)



Best Practices: **Prior to Mobile Device Theft**

Common sense practices are always recommended.

- Be aware of your surroundings
- Keep your mobile device on your person
- Never leave mobile device unattended (in car, on table, etc.)
- Don't lend mobile device to strangers
- Avoid calling attention to yourself and your valuables with loud and interesting ringtones.

Best Practices: **After Mobile Device Theft**

- **Contact the police.**
 - Do not try to retrieve device on your own.
- **Contact your carrier**
 - Give them your MEID, IMEI, or ESN number
 - This will suspend services
 - Prevent unauthorized usage.
 - Initiate an insurance claim.
- **Activate automatic alarm**
 - This will tag the device as stolen or loss.



Best Practices: **After Mobile Device Theft (cont.)**

- **Activate anti-theft or locator software**
 - Using previously installed computer software.
- **Remotely lock your device**
 - Using previously installed computer software.
- **Wipe mobile device clean**
 - Using mobile device theft software.
- **Use a “kill” switch (if available)**
 - This will make your mobile device useless.



Best Solution:
Wireless Device Anti-theft Apps:

- There are many downloadable applications that will help you retrieve or locate your mobile device in the event that it is lost or stolen.
 - Most wireless carrier offer anti-theft software free of charge.

Consumer Outreach (cont. p.2)

In closing, the FCC's Consumer and Governmental Affairs Bureau will continue to work with other government agencies, law enforcement, consumer advocacy groups, and wireless carriers on outreach efforts.

We also welcome outreach opportunities from you.

