

Handset theft – an international view



James Moran, Security Director GSMA

Initiatives to Date

- Blocking of stolen devices on mobile networks
- Sharing of stolen handset data across networks
- Focus on integrity of IMEI necessary to support blocking

These efforts have had some success but there is a clear need for greater industry and government collaboration

- Most initiatives undertaken nationally with narrow view
- Some mandated solutions not designed to combat theft
- Lack of intelligence and handset theft level statistics
- Some governments undermining anti-theft measures
- Black markets continue to exist and thrive
- Lack of legislation and enforcement
- Need to look beyond the obvious and identify new approaches



Kill Switch

Kill Switch

- Politicians have demanded a “kill switch” for stolen phones for some time – they believe it is a panacea
- There has been no definition of what they want
- Complex to implement - difficult to secure and allow re-enablement, need to establish rightful owner, etc.
- Legislation proposed in the USA highlights conflicting requirements and demands:
 - Minnesota
 - Illinois
 - California
 - US Senate
- Need for harmonised and industry set of requirements that a ‘kill switch’ solution should satisfy



Manufacturer Offered Solutions

- Being introduced as standard on many handsets
- Privacy concerns if misused



Find My iPhone

If you lose your iPhone, help is only a tap away.

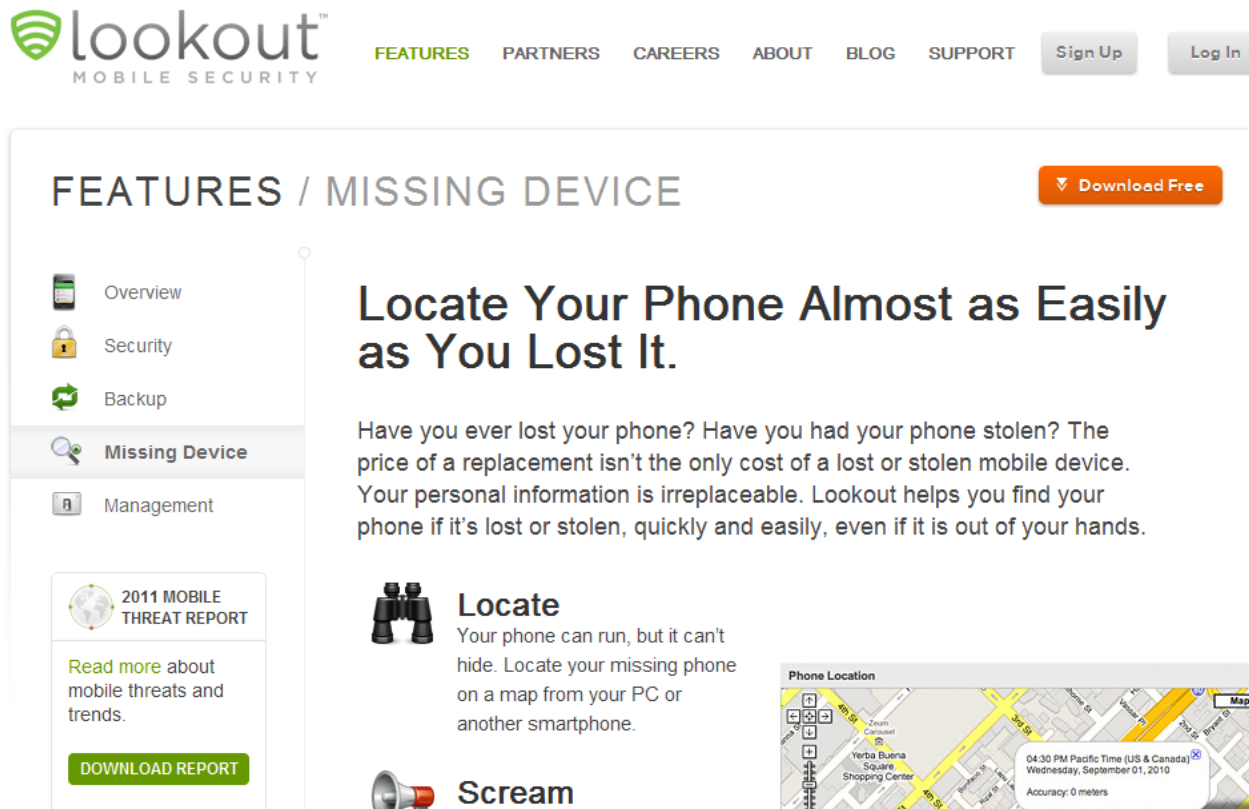
You take your iPhone everywhere. Which means you might leave it anywhere. Whether it's at the office in a conference room or under a pillow on your couch, chances are it won't be lost for long.



- What good is it if your phone appears abroad?

3rd Party Offered Solutions

- Traditional AV vendors can finally add real value
- Packaged, holistic apps:



The screenshot displays the Lookout Mobile Security website. The header includes the Lookout logo, navigation links (FEATURES, PARTNERS, CAREERS, ABOUT, BLOG, SUPPORT), and buttons for Sign Up and Log In. The main content area is titled 'FEATURES / MISSING DEVICE' and features a 'Download Free' button. A sidebar on the left lists navigation options: Overview, Security, Backup, Missing Device (selected), and Management. Below the sidebar, there is a section for the '2011 MOBILE THREAT REPORT' with a 'DOWNLOAD REPORT' button. The main text area is headed 'Locate Your Phone Almost as Easily as You Lost It.' and contains a paragraph about the cost of a lost phone and the service's ability to find it. Below this text are two icons: binoculars for 'Locate' and a megaphone for 'Scream'. A map titled 'Phone Location' shows a specific location in Verba Buena Square Shopping Center with a timestamp and accuracy.

lookout™
MOBILE SECURITY

FEATURES PARTNERS CAREERS ABOUT BLOG SUPPORT Sign Up Log In

FEATURES / MISSING DEVICE [Download Free](#)

Overview
Security
Backup
Missing Device
Management

2011 MOBILE THREAT REPORT
[Read more](#) about mobile threats and trends.
[DOWNLOAD REPORT](#)

Locate Your Phone Almost as Easily as You Lost It.

Have you ever lost your phone? Have you had your phone stolen? The price of a replacement isn't the only cost of a lost or stolen mobile device. Your personal information is irreplaceable. Lookout helps you find your phone if it's lost or stolen, quickly and easily, even if it is out of your hands.

Locate
Your phone can run, but it can't hide. Locate your missing phone on a map from your PC or another smartphone.

Scream

Phone Location
Verba Buena Square Shopping Center
04:30 PM Pacific Time (US & Canada)
Wednesday, September 01, 2010
Accuracy: 0 meters

GSMA Requirements

- To successfully combat mobile device theft will involve;
 - Device Owners – ensuring the safe storage and use of their device and take action once it is missing
 - Device Manufacturers – provide anti-theft tools
 - Network Operators – provide support for device anti-theft features
- Owner control must be provided in the event a device is lost or stolen. Necessary features include;
 - locate a lost device,
 - wipe data,
 - deactivate and render the device unusable, and
 - reactive and restore the device once retrieved
- 17 requirements designed to provide the widest possible choice for manufacturers, operators and 3rd party software and hardware suppliers to innovate and address the problem of device theft



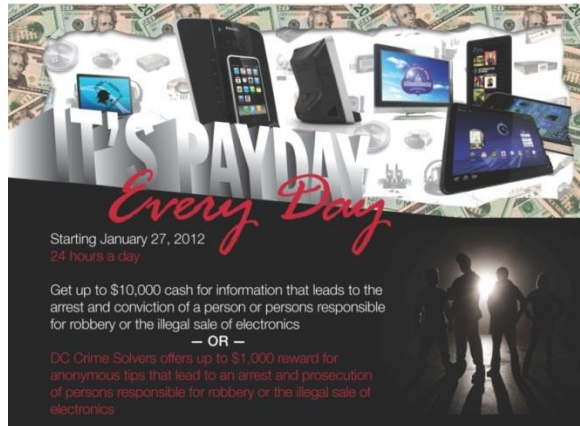
USA



US Industry Initiatives Since 2012

- Apr 2012 “Smartphone Anti-Theft Voluntary Commitment” announced by CTIA committed to
 - Implement databases to prevent use of stolen smartphones
 - Educate consumers on available security features, applications and ant-theft protections and preventative measures
- May 2012 “Analysis and Recommendations for Stolen Mobile Device Issue in the United States” published by GSMA North America decided to block device and share data
- Nov 2103 all top 4 US carriers connected to GSMA IMEI Database
- Apr 2014 – “Smartphone Anti-Theft Voluntary Commitment” released by CTIA agreed the following
 - Devices manufactured after Jul 2015 contain free anti-theft tools
 - Operators to permit anti-theft tools to be preloaded or downloadable

Public and Consumer Awareness



IT'S PAYDAY Every Day

Starting January 27, 2012
24 hours a day

Get up to \$10,000 cash for information that leads to the arrest and conviction of a person or persons responsible for robbery or the illegal sale of electronics
— OR —
DC Crime Solvers offers up to \$1,000 reward for anonymous tips that lead to an arrest and prosecution of persons responsible for robbery or the illegal sale of electronics

REWARD HOTLINE
202-727-9099
24 HRS • 7 DAYS • ALL FREE
GIVE YOUR TIP • GET PAID

ANONYMOUS TEXT
50411

Have you overheard someone bragging about robbing people? Do you know a place where stolen goods are being sold? Has someone tried to sell you the latest hot phone on the street? Put them on blast and you could get up to **\$10,000** cash for your information.

EVERY DAY ALL DAY

the
METROPOLITAN POLICE DEPT
and you

Taking the profit out of crime.

Get more on
rewards at mpdc.dc.gov/rewards



National Crime Prevention Month

Be Cautious When Leaving the Store with Your New Gadgets



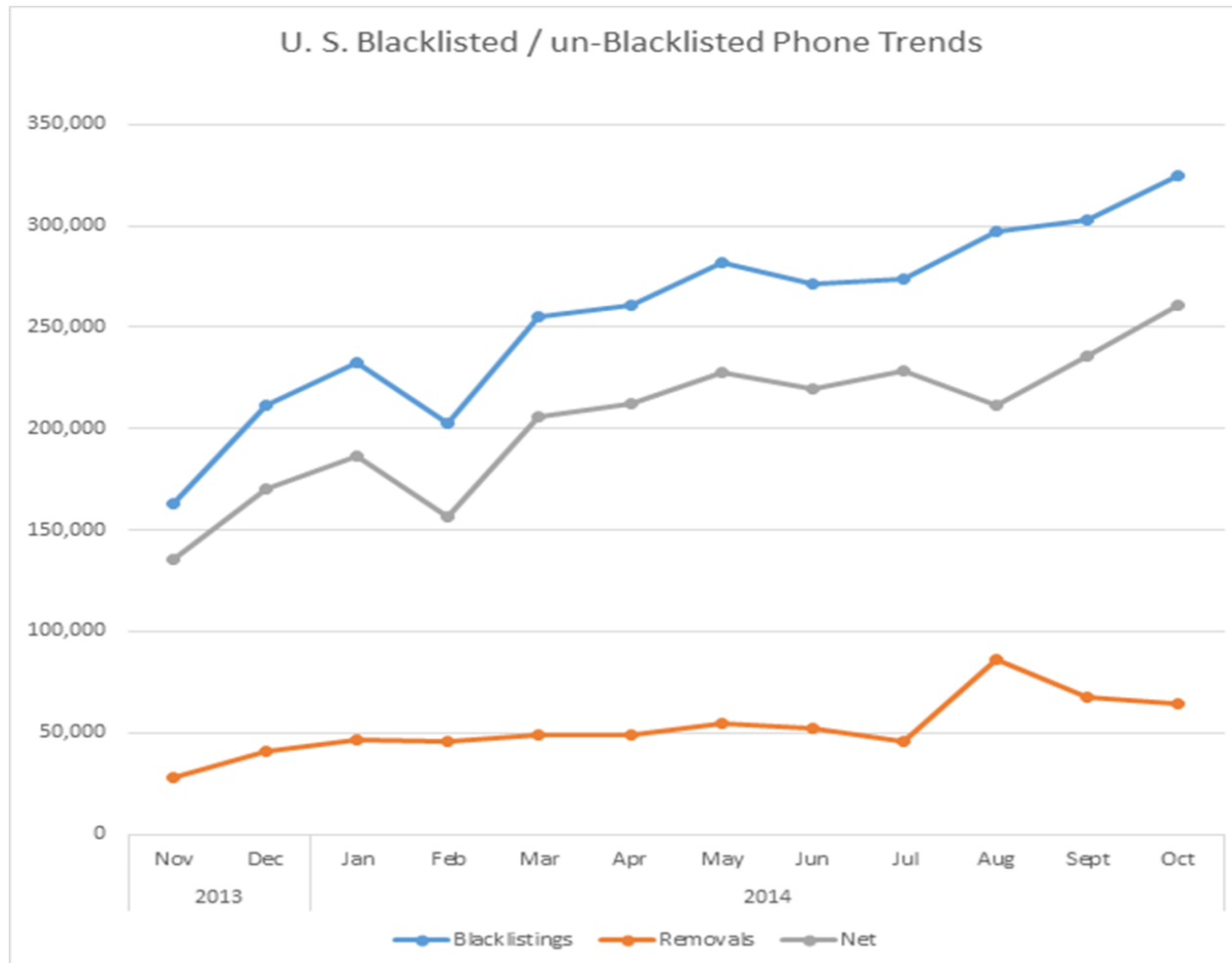

The officers of the Metropolitan Police Department would like to remind members of the public to be cautious when making electronic purchases, particularly on days of new releases of popular devices and gadgets. If you have plans to make a major purchase of a popular computer, tablet, or phone, please remember these important safety tips:

1. If an **online tracking system** is available for your device, get the extra assistance in the store for setup before exiting the store.
2. **Don't be distracted** as you exit local cell phone stores and other electronic specialty stores that sell these items. Be deliberate as you exit these stores, concealing your purchase(s) and focusing on getting to your next destination. Cell phones and other music devices are major distractions when in use.
3. **Report suspicious people.** *Inside a store:* Do you notice people who are paying more attention to the purchases being made, rather than checking out new products? *Outside a store:* Do you see suspicious people standing at or near the exit for no real purpose? Report these behaviors to police.
4. **Try to shop with a friend.** Most victims who report crimes that involve snatching new products are people who have shopped alone. If you have an elderly parent, please make preparations to accompany him or her to make these kinds of purchases or suggest ordering them online.
5. Never hesitate to **point out suspicious activity** or people to local officers or security guards. Remember the "See Something, Say Something" campaign and dial 9-1-1 if you need an officer dispatched to your location.

Office of Community Outreach and
Patrol Services & School Security Bureau



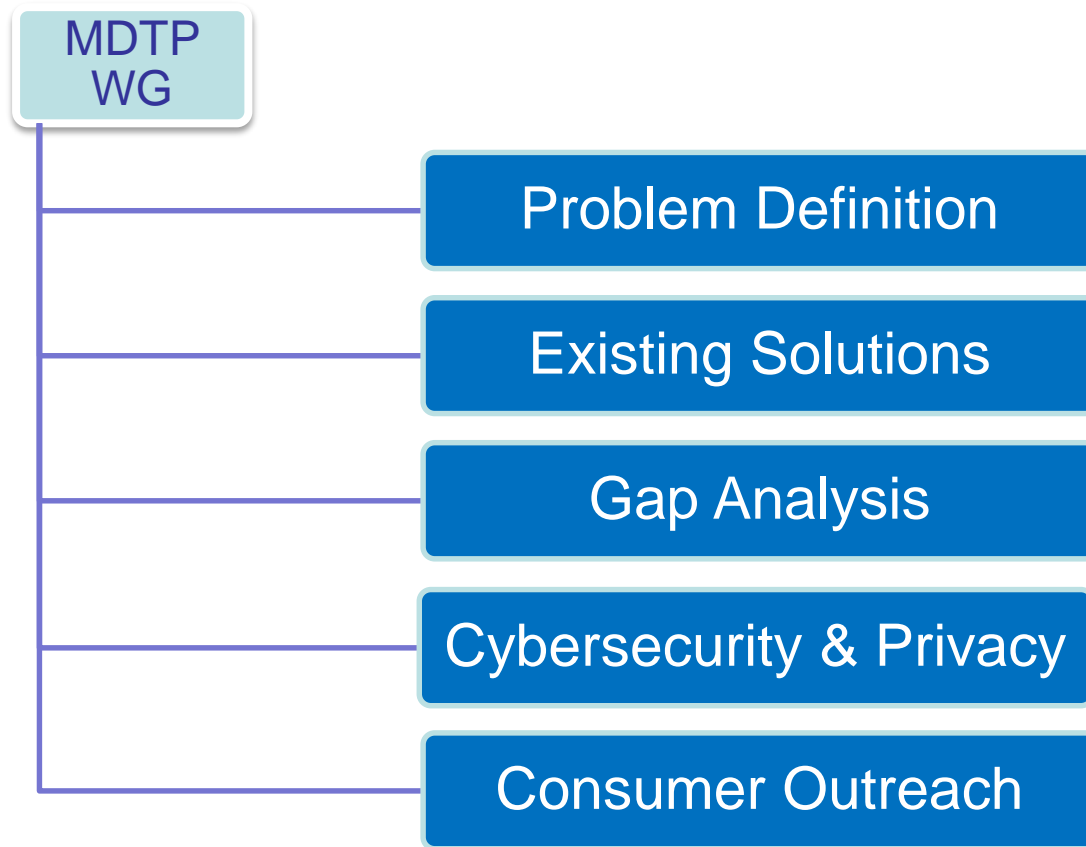
USA Blacklisting Volumes



FCC – Mobile Device Theft Prevention Working Group

- FCC workshop held in Washington DC in June 2014 to discuss solutions rather than the problem
- Working Group created to develop recommendations by end 2014 to mitigate device theft.
- Specifically tasked to:
 1. Define key terms that are central to this matter
 2. Develop best practices for consumer engagement and education
 3. Explore stakeholder coordination and data sharing
 4. Ensure appropriate considerations of cybersecurity concerns
 5. Identify gaps with existing solutions
 6. Analyze the need and value of new technical and operational solutions
 7. Identify standards organizations and industry fora to implement solutions.

MDTP WG Structure



MDTP WG Recommendations

- Recommendations being formulated that fall into the following four areas:
 - Actionable Recommendations for the FCC
 - Guidelines to Law Enforcement
 - Guidelines to Industry
 - Further Work
- Recommendations will focus on:
 - Need for all stakeholders to engage to develop a national strategy
 - Allowing industry to identify and evolve technical solutions
 - Promoting greater use of device blocking and data sharing solutions
 - Continued development and promotion of device based solutions
 - Increased consumer outreach and education on tools and prevention
 - Greater police awareness of device theft
 - Introduction of IMEI checks at retail outlets
 - Facilitating consumer IMEI checks
 - Measuring and reporting theft levels



Regulatory Initiatives

2011 CITEL Recommendation

“measures have proven insufficient to combat this illicit industry”

- **Introduce blacklisting** of stolen devices in individual countries
- **Exchange blacklist data regionally** using solutions such as **IMEI Database**
- Raise public awareness of handset theft and the need to buy from reputable sources
- States to **criminalise IMEI changing** or other circumvention of blacklisting
- States to better control import and movement of mobile handsets
- Sellers of handsets to only buy and provide for sale those with a secure IMEI
- Operators to **report instances of IMEI security weakness** for investigation

“criminal organizations profiting from this business take advantage of the absence of information exchange and of blockage at the international level”



ORGANIZACION DE LOS ESTADOS AMERICANOS
ORGANIZATION OF AMERICAN STATES

Comisión Interamericana de Telecomunicaciones
Inter-American Telecommunication Commission



New ITU Draft Resolution



RESOLUTION COM5/5 (BUSAN, 2014) - Assisting Member States to combat and deter mobile device theft

- **Recognises** the issue and that individual countries have taken initiatives and that
- **Concerned** that the rate of mobile device theft remains high despite efforts
- **Aware** that industry has been developing different technological solutions and governments have been developing policies to address the problem
- **Resolves** to explore all ways and means to combat and deter mobile device theft,
- **Instructs** the ITU to:
 - compile information on best practices,
 - consult with stakeholders to identify existing and future technological measures
 - provide assistance to reduce mobile device theft and the use of stolen mobile devices in their countries
 - Have Secretary General report annually to the Council on progress
- **Invites** Member States and Sector Members to contribute to the studies



Looking at the Future

- Need for industry and government engagement and collaboration rather than imposing regulations and solutions
- Grater emphasis on collective efforts required to ensure all parties and countries play their role
- Opportunity to take stock and critically assess successes and failures
- Need for statistical data to be gathered and shared to enable analysis
- Learn from what has worked well and what has not and identify why
- Embrace emerging technologies and solutions to bridge gaps



Thank you for your attention

Any Questions?

James Moran
Security Director, GSM Association
jmoran@gsma.com