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

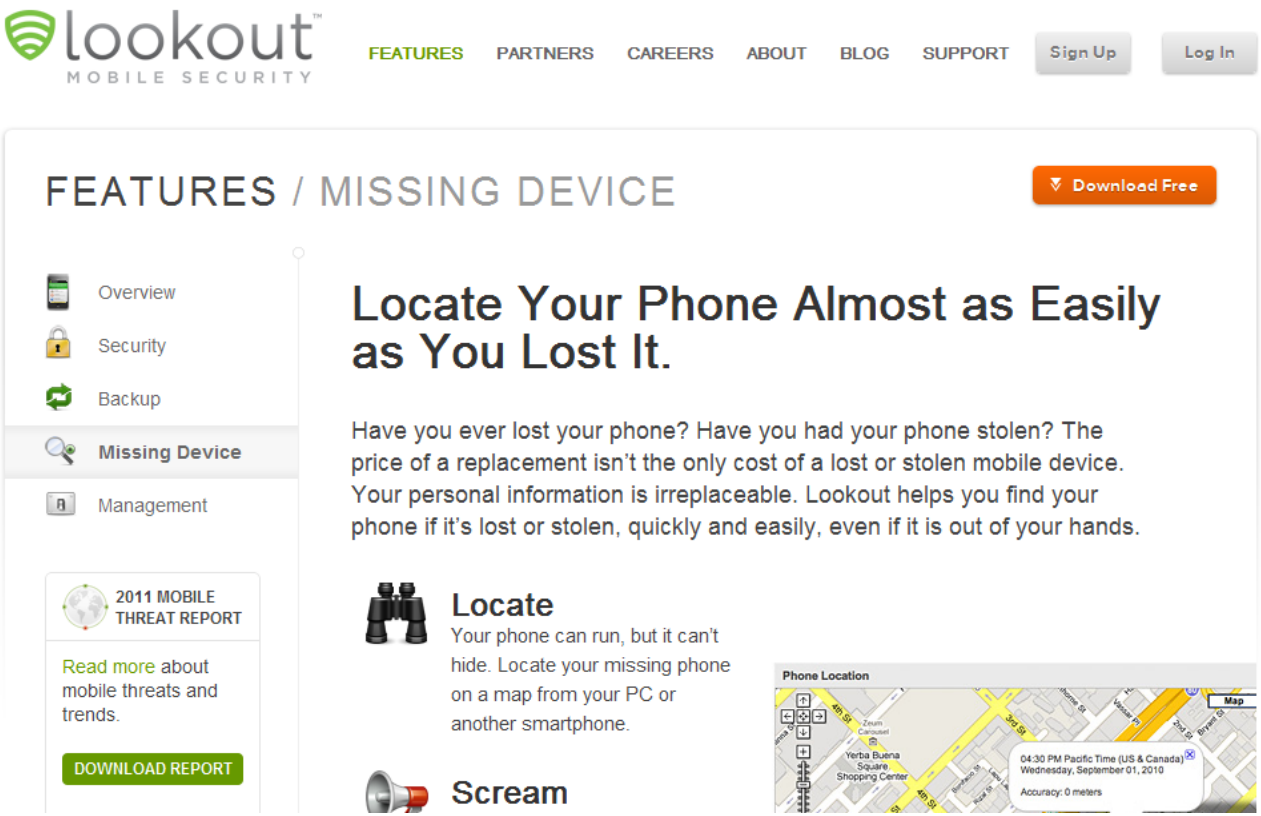
Manufacturer Offered Solutions

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

- What good is it if your phone appears abroad?

3rd Party Offered Solutions

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



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

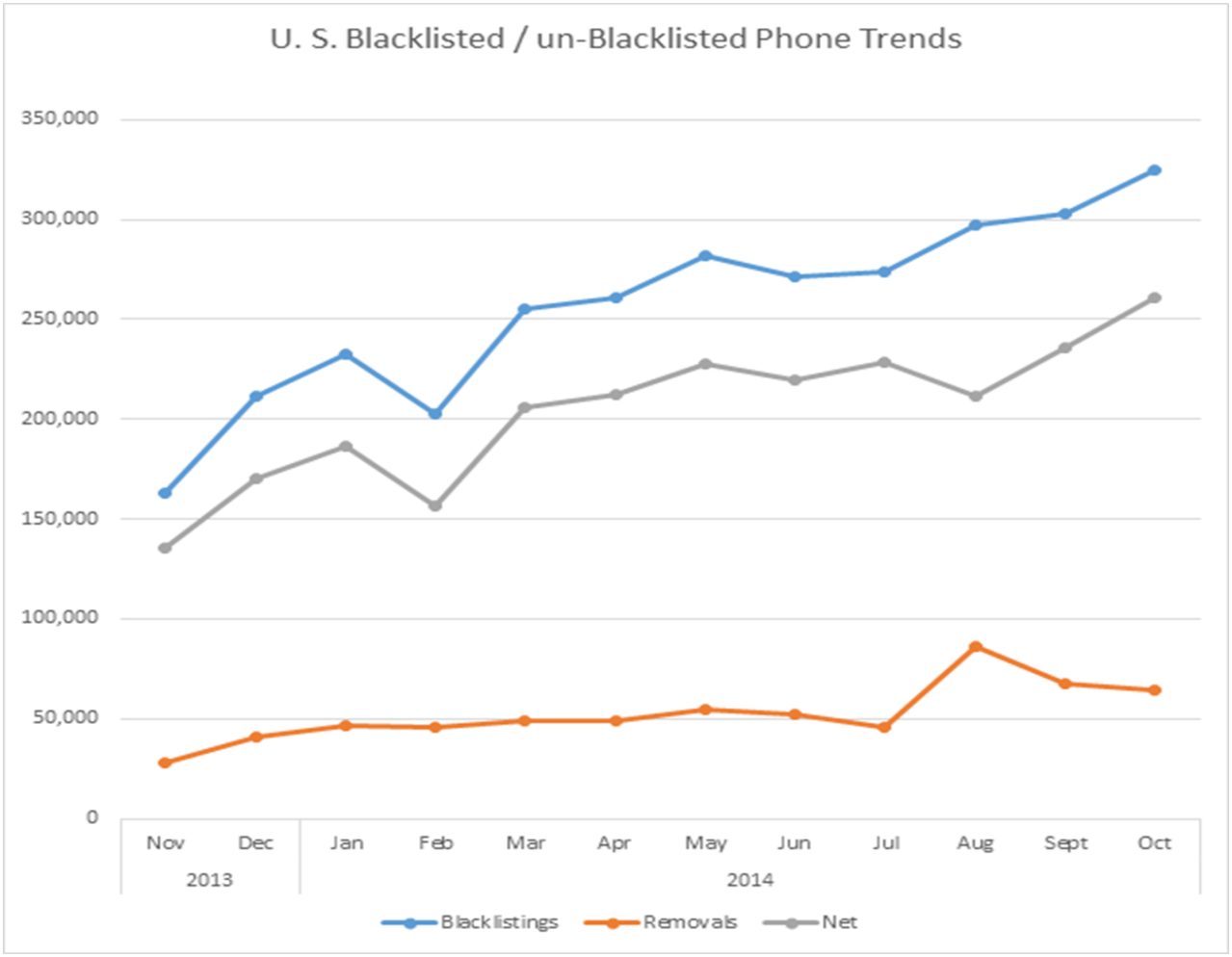
USA

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

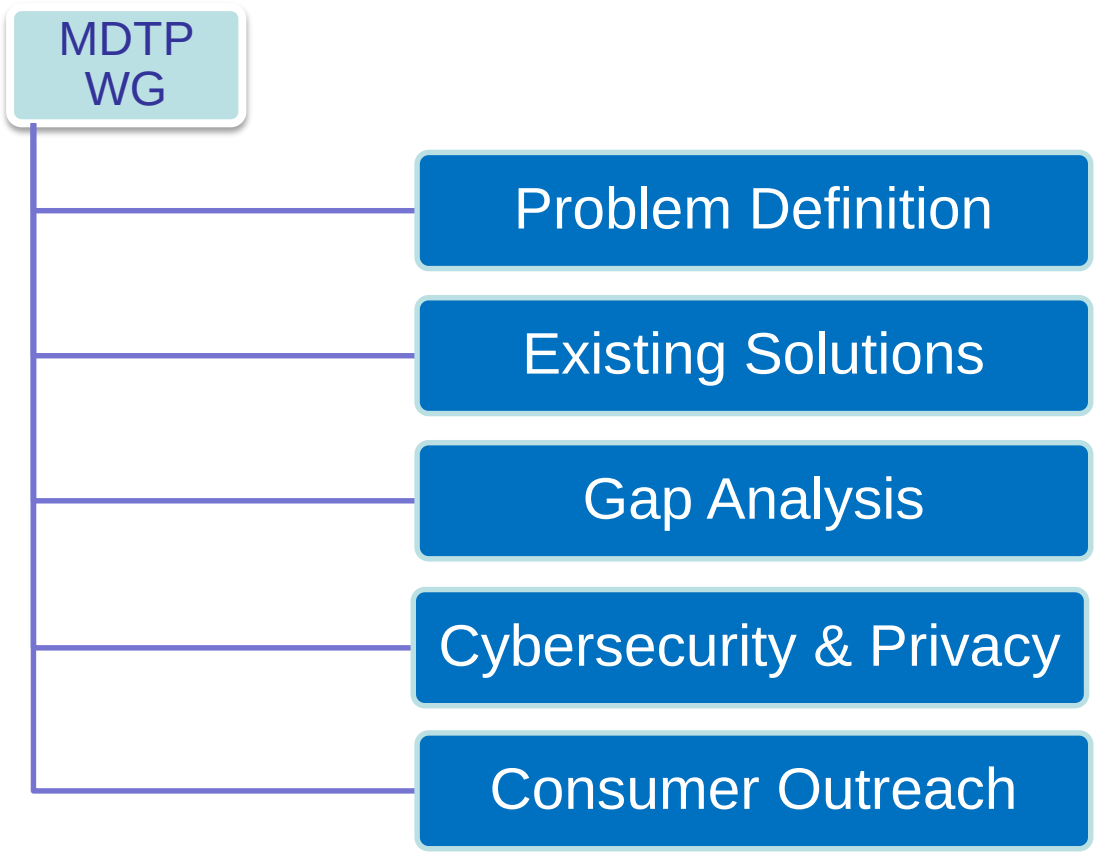
USA Blacklisting Volumes



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 important 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