Mobile Device Theft in Latin America

July 23, 2018
Contents

Device Theft in Latin America
  A Growing Problem

Anti-Theft Tools
  IMEI Blocking and Technical Tools

Existing Initiatives in Latin America
  Wide Variety of Policies

Technology Offers a Supplemental Solution
  Key Recommendations
Device Theft: A Growing Problem

As smartphones have become more prevalent in Latin America, device theft has similarly increased.

Sources:
La Nacion, “Por día se roban 5000 celulares en la Argentina” July 26, 2016, available here
CRC, “Condiciones Regulatorias para el Control del Uso De Equipos Terminales Móviles Hurtados y/o Extraviados”, June 2011, pg. 3, available here
Anti Device Theft Tools

- Latin American countries were early adopters of policies to identify stolen or otherwise unauthorized devices and prevent them from connecting to networks.
  - These include IMEI blocking approaches such as whitelists and blacklists.
- Devices that cannot be used on a mobile network are less valuable, thereby reducing the incentive for device theft.
- Technical solutions have been widely implemented by manufacturers
Blacklists

Disconnecting stolen devices

Centralized list of excluded devices, i.e. a blacklist, which contains the IMEIs of devices reported as stolen or lost.

Operators subsequently block devices with reported IMEIs from connecting to their networks.

IMEIs of stolen devices reported to a national database. National database is synchronized with the GSMA’s global database.

The GSM Association (GSMA), a global association of mobile operators, has been compiling a global blacklist database since 1996.

The GSMA IMEI database contains more than 39 million entries reported by countries in the Americas.

In 2014, there were fewer than 1 million IMEIs in this database.

Rapid growth is due to greater regional adoption and increases in both thefts and the quantity of mobile devices in Latin America.

Source: TMG Based on GSMA data. Also, see CITEL, PCC.I/Doc 4477/17 (XXXI-17) “Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017” July 2017.
Blacklists in Action

Example: Colombia and Brazil

- Device Stolen
- IMEI blocked & added to Colombian blacklist
- Added to National blacklist
- Added to GSMA global database
- Downloaded to Brazilian database
- Brazilian operators block downloaded IMEI
Whitelists

Preventing stolen devices from connecting

- Whitelists list devices are approved to connect to a network. Unlisted devices cannot connect to the network.

- Devices must meet specific criteria and complete registration, creating additional obligations for both device importers and end users.

- Requires registration of any devices to be sold within national borders.

- Higher degree of variation between countries with whitelists than blacklists and lower potential for regional coordination.
Whitelists

Example of a whitelist in action: Colombia

- Added to national whitelist
- Operator allows device to connect to network

Periodic download of whitelist
Technical Solutions

Devaluing stolen devices

- CTIA Smartphone Antitheft Voluntary Commitment undertaken by industry to address the issue in the United States.
- The Commitment was signed by 16 operators, manufacturers, and other U.S. stakeholders, and was fulfilled by 2015.

- Such approaches have been shown to make a significant impact on the rate of device theft:
  - London thefts dropped 38% after introduction of kill switch
  - New York City thefts dropped 16%; and
  - San Francisco thefts dropped 27%.

- Technical approaches to combatting mobile device theft do not rely upon blocking or approving IMEIs and require minimal regulatory involvement.

Sources:
## Pros and Cons of Anti Theft Approaches

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blacklists</strong></td>
<td>• Less user inconvenience than whitelists.</td>
<td>• Little evidence indicating that blacklists reduce or prevent theft.</td>
</tr>
<tr>
<td></td>
<td>• Can be coordinated regionally and even globally.</td>
<td>• Not being implemented uniformly across the region, creating harmonization issues.</td>
</tr>
<tr>
<td></td>
<td>• Already widely implemented and accepted by regulators and operators.</td>
<td>• Rely on accurate reporting, which rarely occurs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Thieves have developed countermeasures (duplication and alteration of IMEIs, moving stolen devices to a different country).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High database maintenance and infrastructure requirements and costs.</td>
</tr>
<tr>
<td><strong>Whitelists</strong></td>
<td>• Can cover devices with unformatted or duplicated IMEIs, which are types of fraud sometimes ignored by blacklists.</td>
<td>• Registration requirements inconvenience users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implementation difficulty due to requirement that existing phones be added to whitelist.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not being implemented uniformly across the region, creating harmonization issues and fragmentation of regional device market. Can impede cross-border movement of devices, including legitimate movement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Often combined with import and export requirements that are onerous for businesses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Require a high level of database accuracy in order to be effective.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Effectiveness is unproven.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High initial costs associated with infrastructure necessary to process, record, and store information on all devices in country.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High ongoing costs associated with staff and infrastructure needed to record data on all imported devices.</td>
</tr>
<tr>
<td><strong>Technical Solutions</strong></td>
<td>• Prevent stolen device from connecting to network.</td>
<td>• Only works on smartphones, not feature phones. Latin America has a significant percentage of feature phones.</td>
</tr>
<tr>
<td></td>
<td>• Can erase personal data on stolen devices, protecting user privacy.</td>
<td>• Often requires user opt-in.</td>
</tr>
<tr>
<td></td>
<td>• Easily accessible as downloadable or pre-installed apps.</td>
<td>• Does not work if the phone is turned off or is in airplane mode.</td>
</tr>
<tr>
<td></td>
<td>• User-controlled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does not require cumbersome reporting processes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No cost to governments for database maintenance or adoption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No issues with cross-border or regional harmonization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Easily reversible in cases where device is recovered.</td>
<td></td>
</tr>
</tbody>
</table>
Existing Initiatives in Latin America

**Blacklists**
- Argentina
- Brazil
- Costa Rica
- Dominican Republic
- Mexico
- Paraguay

*Focused only on homologation*

**Whitelists**
- Chile*
- Colombia
- Ecuador
- Honduras**
- Peru

*Whitelists always accompanied by blacklists*

**Implementation in progress**
Existing Initiatives II
Examples of variation between countries

Peru
- Devices must also be linked to national civil registry entry of device owner.

Chile
- Whitelist addresses homologation before sale of imported devices, but is not designed to be updated as devices are stolen.

Ecuador
- User must report theft for blocking process to begin.

Brazil
- Police may also initiate a stolen device report.
Effectiveness of the current approach

- A blacklist’s success depends on robust and accurate reporting practices, which are difficult to achieve in countries where the majority of crimes go unreported.
  - In Colombia, for example, only an estimated 4% of phone thefts were reported to the police in the first half of 2017.
  - In Brazil, a recent survey found that only 51% of victims of cell phone theft notified the police.
  - In Peru, despite the implementation of blacklists and whitelists, approximately 6,000 devices are stolen each day, or an average of 250 devices per hour.

- Thieves have discovered workarounds to the blacklist system, especially by tampering with IMEIs and/or selling stolen devices in neighboring countries.

Sources:
Technology Offers a Supplemental Solution

- Successful
  - Proven to reduce device theft.

- Low Cost
  - No cost to governments, operators, or consumers.

- Frees Resources
  - Allows law enforcement to refocus resources.

- User Controlled
  - Industry-led, user-controlled solution.

- Available Today
  - No lengthy implementation period.

- Boosts Sales
  - Anti-theft as smartphone selling point.

- Easily Reversible
  - Easy to reverse when device recovered.
Improving Blacklists

Complementing a technical solution

In order to maximize the benefits of a blacklist, policy makers must strive for:

- Greater Harmonization and Adoption
- Global Reach
- Improved Accuracy

Result: Greater Effectiveness
Blacklists were never intended to solve the device theft problem on their own. They are part of an effective solution that includes encompasses law enforcement, improved administrative systems to increase accuracy of databases, and consumer education. Even with improvements, blacklist databases remain a potential point of failure for any country’s approach to reducing device theft because any failure or corruption of the data reduces its value as a tool in the fight against device theft.

Keys to a Successful Approach

01  Law Enforcement
02  Improved Accuracy
03  Consumer Education
Consumer Education

Improving effectiveness through greater awareness

- Consumer involvement is key to the success of any measures to combat device theft. Both IMEI blocking measures, such as blacklists, and technical solutions like a kill switch require user participation to be effective.
  - Anti-theft technology often available as “opt-in.”
  - Accurate and timely reporting key to accuracy of blacklist databases.
  - Consumers need to be aware of the importance of buying devices with valid IMEIs.

This mechanism allows users to check the history of a device’s IMEI that they own or are considering purchasing against the GSMA blacklist. Since its inception in 2014, the campaign has had 13 launches around the region and 18 public announcements of industry initiatives.

GSMA, “GSMA Device Check” official website, available here. Accessed October 2017
Key Findings and Recommendations

- It is widely accepted that solely blocking devices based on IMEI numbers is likely to be not fully effective as a solution.
- Neither blacklists nor whitelists resolve the issue of device theft totally, and both involve costs borne by some combination of regulators, operators, and users.
- Technological solutions have been shown to reduce theft in other regions of the world.
- Technology-based solutions implemented by major manufacturers can make device theft less lucrative without requiring a commitment of additional public funds or imposing costly burdens on consumers and businesses.
- Given these limitations, Latin America would be best served by an approach that:
  1. increases the visibility and use of technology-based solutions that,
  2. is complemented by improved blacklists, and
  3. updates the legal system to criminalize key activities involved in the collection, modification, and dissemination of stolen devices.

CITEL, PCC.I/Doc. 2311 (XVII-11) “GSMA Resources and Position to Support Regional Front to Combat the Theft of Mobile Terminal Equipment,” September, 2011