Mobile Device Theft in Latin America

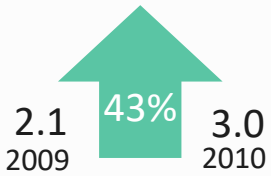
July 23, 2018

Contents

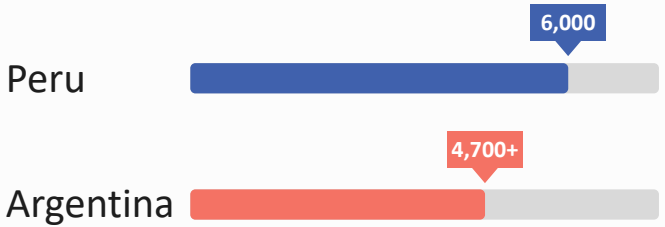
Device Theft: A Growing Problem

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

Increase in smartphone theft in Colombia (millions)



Number of smartphones stolen per day



Sources:
La Nacion, “Por dia se roban 5000 celulares en la Argentina” July 26, 2016, available here
La Republica, Perú. “Bloqueo de celulares con pocos resultados: cada hora roban 250 equipos,” available here Accesed February 2018
Attorney General of Colombia, “Press Release: El bloqueo de los IMEI de los celulares no está funcionando,” August 4, 2017, 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

Blacklists | **Whitelists** | **Technical Solutions**

- 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

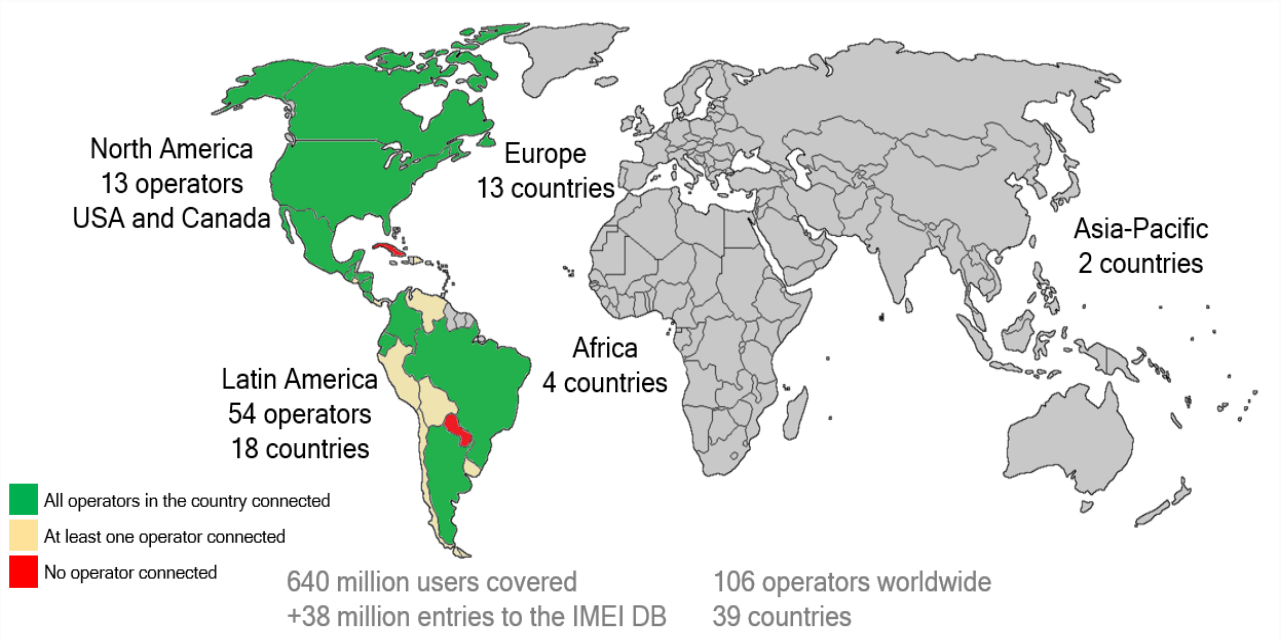
Blacklists

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.

See 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.

GSMA Database

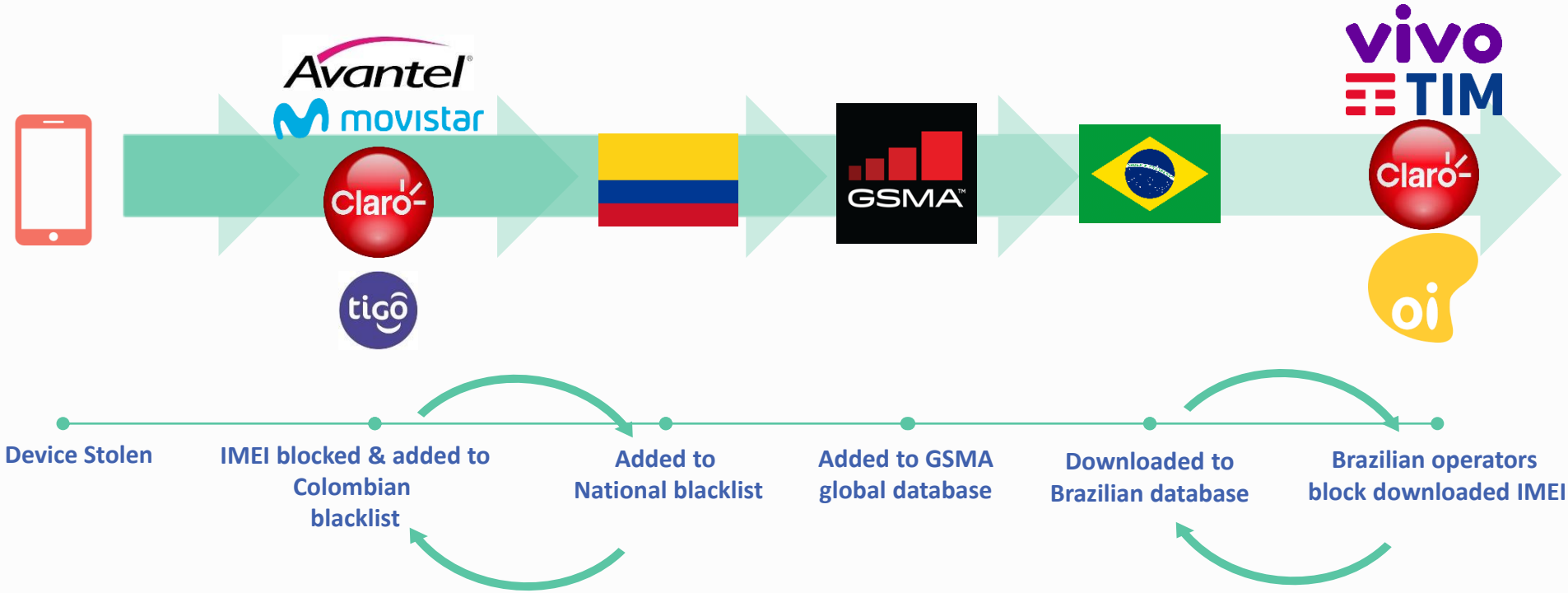


- The GSMA IMEI database contains more than 39 million entries reported by countries in the Americas
- In 2014, there were fewer than 1 million IMEIs in this database.
- Rapid growth is due to greater regional adoption and increases in both thefts and the quantity of mobile devices in Latin America.

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**



Whitelists

Preventing stolen devices from connecting

- Whitelists list devices are approved to connect to a network. Unlisted devices cannot connect to the network.
- Requires registration of any devices to be sold within national borders.
- Devices must meet specific criteria and complete registration, creating additional obligations for both device importers and end users.
- Higher degree of variation between countries with whitelists than blacklists and lower potential for regional coordination.

Whitelists

Example of a **whitelist** in action: Colombia

Whitelisted Device (Connected)

New Device (no connection)

Added to national whitelist

then

Operator allows device to connect to network

movistar

tigo

Claro

Avantel

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:
CTIA, "Smartphone Anti-Theft Voluntary Commitment," April 2014, available here. Accessed October 2017
San Francisco District Attorney, "Press Release: A.G. Schneiderman, London Mayor Johnson and D.A. Gascon Welcome Dramatic Global Drop in Smartphone Thefts Following Introduction of Kill Switch" February 11, 2015, available here. Accessed October 2017.

Pros and Cons of Anti Theft Approaches

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

Existing Initiatives in Latin America

Whitelists always accompanied by blacklists

*Focused only on homologation
**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:
Panorama Mobile Time/Opinion Box, "Roubo de celulares no Brasil," July 2017. Available for download here. Accessed October 2017
El Tiempo, "Colombia es el país de la región con mayor robo de celulares," August 8, 2017, available here. Accessed October 2017.

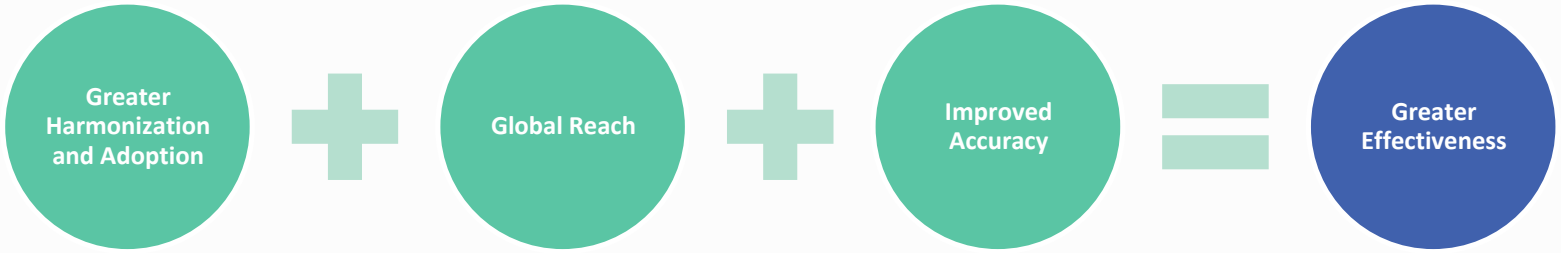
Technology Offers a Supplemental Solution

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:



Improving Blacklists II

A Holistic Approach

Keys to a Successful Approach

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.

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.

GSMA Device Check

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

Geraldo Neto
geraldo@tmgtelecom.com