Mobile Device Theft in Latin America

Current policies and issues

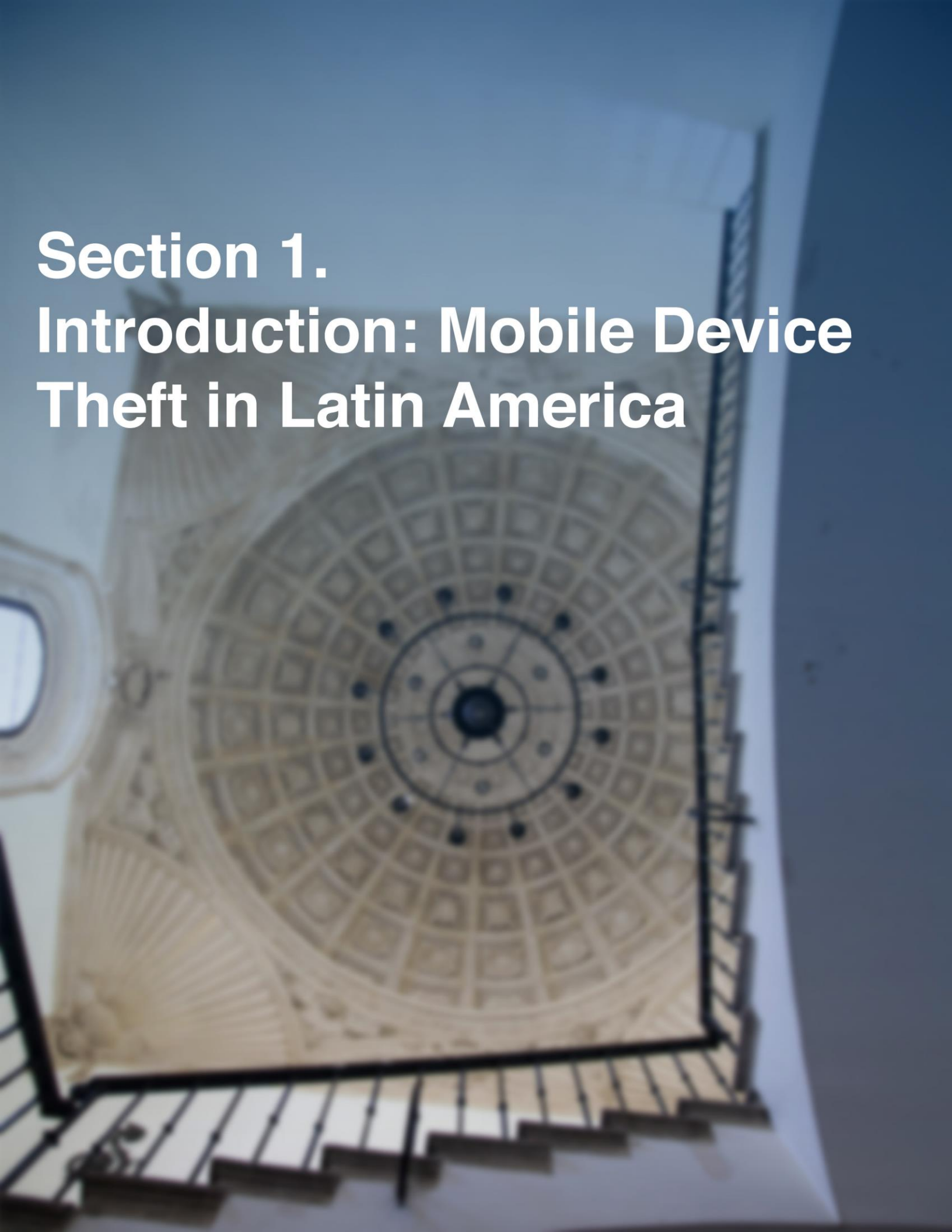
Comments can be addressed to reports@tmgtelecom.com.

1600 Wilson Blvd., Suite 710

Arlington, VA 22209 USA

November 2017

Table of Contents



Section 1. Introduction: Mobile Device Theft in Latin America

1 Introduction: Mobile Device Theft in Latin America

Mobile device theft has been an issue in Latin America since the inception of the mobile device market.[1] However, the increased adoption of mobile phones, especially after the introduction of smartphones, has led to a rapid rise in mobile device related crime in the region. Between 2009 and 2010, the number of stolen mobile devices grew from 2.1 million devices to 3 million—a 43% increase.[2] Despite efforts to control the issue, it remains pervasive throughout the region. In Colombia, cell phone theft was the fastest growing crime in the first half of 2017,[3] while in Argentina, more than 4,700 phones were stolen each day in 2016.[4]

This growing problem, and the fact that such theft is often accompanied by violence, is recognized by industry stakeholders, regulators, and the public.[5] This has prompted governments in the Americas region to enact policies to combat this issue. Furthermore, regional and international organizations have also introduced initiatives to address it.

Countries in Latin America were early adopters of policies that seek to identify stolen or otherwise unauthorized devices, such as those that authorize only verified, legitimate devices to use a network (known as whitelisting) to address mobile theft. Since 2011, Latin American governments have steadily enacted policies to combat the theft of mobile devices, including the blacklisting and whitelisting of devices based on their International Mobile Equipment Identity (IMEI). Today, more than 18 countries have adopted policies relating to mobile device theft.[6] Many of these countries have taken a broad approach to the issue, targeting not only stolen devices, but also counterfeit and fraudulent ones. Although well-intentioned, these policies have created their own issues, including inconveniencing users and increasing costs to business, while not necessarily effectively reducing theft. In addition, the list-based policies adopted in many countries are not designed to address all aspects of the stolen device market, such as the black market for stolen device components.

This report provides an overview of the measures adopted in the Americas to combat mobile device theft and assesses their effectiveness. Section 2 – Anti-Theft Tools – discusses the primary tools available to combat device theft, and compares their strengths and weaknesses. Section

---

[1] Unless otherwise stated, mentions of mobile device theft refer to theft of devices that have been assigned an International Mobile Equipment Identity number (IMEI) that access mobile telecommunications networks. By nature of the measures adopted, the focus is only on devices with an IMEI that connect to a mobile network. In the popular discourse on this issue by the public and by regulators, the focus is overwhelmingly on mobile phones.

[2] CRC, "Condiciones Regulatorias para el Control del Uso De Equipos Terminales Móviles Hurtados y/o Extraviados", June 2011, pg. 3, available here. Accessed October 2017.

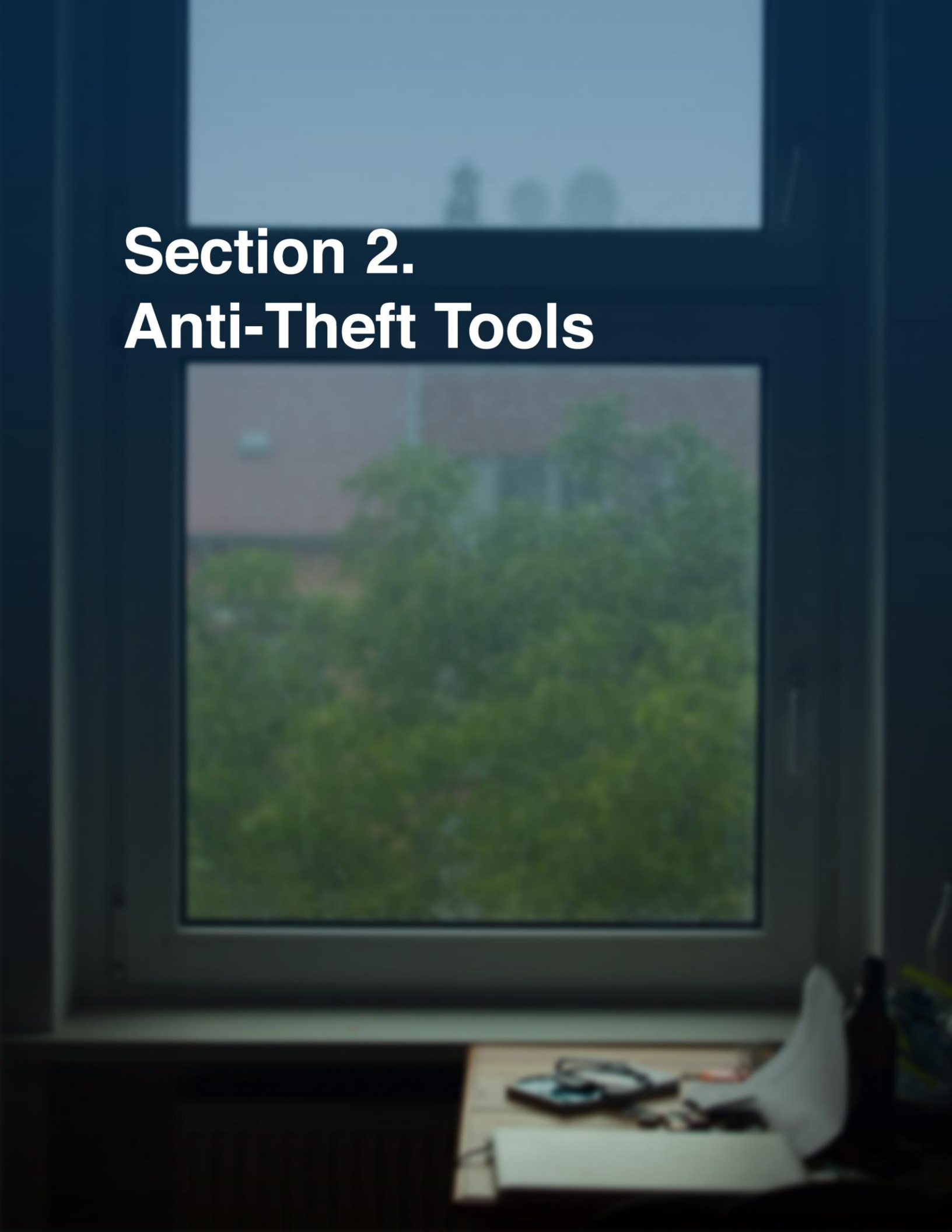
[3] Attorney General of Colombia, "Press Release: El bloqueo de los Imei de los celulares no está funcionando," August 4, 2017, available here. Accessed October 2017.

[4] See La Nacion, "Por dia se roban 5000 celulares en la Argentina" July 26, 2016, available here. Accessed October 2017.

[5] See for example, New York State Attorney General, "Secure our Smartphones," 2014, pg. 11, available here, and El Tiempo, "En video quedó registrado el asesinato de joven misionero en Cali" October 21, 2016, available here. Accessed October 2017.

[6] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.

Existing Initiatives in Latin America – looks more closely at the approaches taken by Latin American governments and the region as a whole to counter device theft, and assesses the effectiveness of such measures. Section 4 – Technology Offers a Better Solution – considers how to improve the effectiveness of anti-theft efforts. Section 5 – Conclusion – summarizes the report's conclusions.



Section 2.
Anti-Theft Tools

2 Anti-Theft Tools

In response to the ongoing problem of mobile device theft, policymakers and industry stakeholders have developed solutions intended to make stolen devices less attractive to thieves and potential buyers. These solutions generally fall into two categories: IMEI-based blocking measures and technical solutions. The former have been widely implemented across Latin America, while technical solutions have, to date, been more prominently employed in North America and Europe.

2.1 IMEI Blocking Measures – Blacklists and Whitelists

While there is regional coordination in the fight against device theft, legislation and policies are enacted on a national level. The result is a complicated milieu of systems, laws, and regulations that approach the same issue in different ways. In general, the systems are based on either a list of blocked devices (blacklist), or a list of allowed devices (whitelist). Some countries also include other categories, such as exported devices.[7]

2.1.1 Blacklists

The initial policies implemented in the region to combat device theft were based on the idea of preventing stolen, fraudulent, or lost devices from connecting to mobile networks. In practice, such an approach relies upon a centralized list of excluded devices, i.e. a blacklist, which contains the IMEIs of devices that were reported by users as stolen or lost. Operators subsequently block devices with the associated IMEIs from connecting to their networks. The concept is that devices that cannot be used on a mobile network are less valuable, thereby reducing the incentive for device theft. The GSM Association (GSMA), a global association of mobile operators, has been compiling a global blacklist database since 1996.[8]

Blacklists typically function on multiple levels. Consumers and/or the police report IMEIs of stolen devices to operators, who then report that information to a national database or otherwise share the data with all operators within the country. The operators then synchronize their databases with the GSMA's global database. Exchange of information with the GSMA database is free for GSMA members and complementary access is often provided to government regulators.[9] Many governments require the exchange of information between operators and the GSMA to happen at least once every 24 hours, and in many cases, more frequently. In this way, a phone reported as stolen, for instance, in Brazil can be blocked from connecting to the network in neighboring Argentina, undermining the transnational trade in stolen devices. However, blacklists function best when they are harmonized with respect to their contents, ensure accuracy of the information they contain, and are widely – if not uniformly – adopted.

---

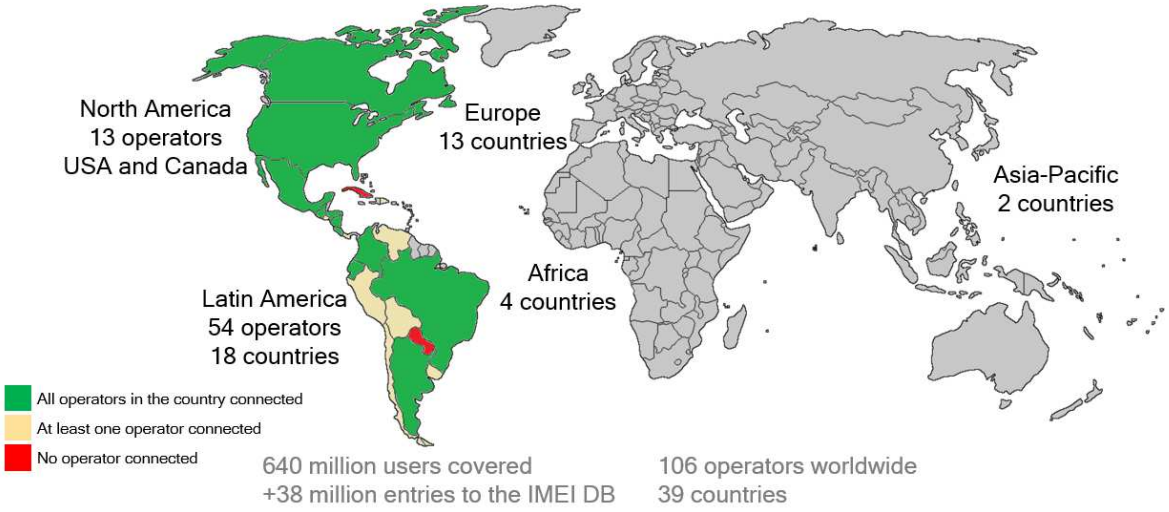
[7] For example, Peru maintain lists of exported devices. See chapter III, art.7, Legislative Decree 1338/2017, available here. Accessed October 2017.

[8] 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.

[9] See GSMA, "Coloured Lists" available here, and GSMA, "Accessing the IMEI Database" available here. Accessed October 2017.

Blacklists have been widely implemented throughout Latin America, but are not in use by all operators in the region, which would make them most effective. Operator subscriptions to the global GSMA database of blacklisted IMEIs are shown in Figure 1. Within Latin America, subscriptions to the GSMA's database rose rapidly after a 2011 resolution by the Inter-American Telecommunications Commission (CITEL) promoting measures to fight device theft, as discussed in Regional Initiatives.[10] Part of the Organization of American States, CITEL addresses telecommunications-related issues, and is comprised of both governments in the Americas and associate members from the private sector. Today, operators in the Americas constitute the majority of those involved with the GSMA blacklist.

Figure 1: Worldwide subscriptions to the GSMA blacklist

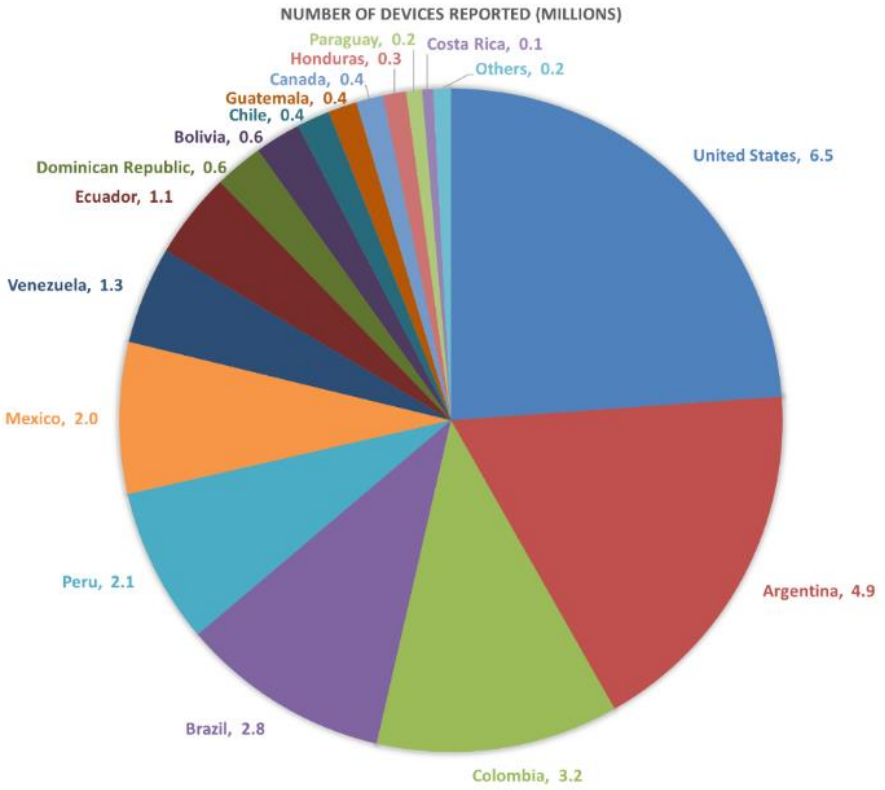


Source: TMG based on GSMA data

Currently, the GSMA IMEI database contains more than 39 million entries reported by countries in the Americas.[11] The database has grown rapidly due to greater regional adoption of, and increases in, both thefts and the quantity of mobile devices in Latin America. In 2014, there were fewer than 1 million IMEIs in this database.[12] Figure 2 shows the number of blacklisted IMEIs as reported by each country in the region. After the United States, Argentina and Colombia have the highest number of IMEIs reported, with 4.9 million and 3.2 million, respectively.

[10] CITEL, PCC.I/RES. 189 (XIX-11) "Regional Measures to Combat the Theft of Mobile Terminal Devices," September, 2011, available here.
[11] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.
[12] Id.

Figure 2: Number of IMEIs reported as lost or stolen by each country in the region



Source: TMG based on GSMA[13]

Blacklists bring certain benefits that continue to make them attractive to policymakers. For example, the implementation of a blacklist is relatively convenient for users, only requiring them to report lost or stolen devices. The only other end-user interaction should occur if a legitimate device is added to the blacklist and the user needs to resolve the mistake. Blacklists can also be designed to be coordinated between not only different operators, but also countries. The widespread use of blacklists and the availability of, for example, the GSMA's global blacklist, create an established system that appeals to policymakers.

However, there are also drawbacks to the use of blacklists, and broadly, there is little evidence to date demonstrating the effectiveness of blacklists in reducing mobile device theft, as discussed further in Section 3.5 – Effectiveness of the Current Approach**.**

On a national level, the manner in which blacklists are used to combat device theft may vary, creating a non-uniform and inharmonious implementation. Some countries, such as Brazil, apart from allowing stolen/lost devices to be reported via operators, also allow law enforcement to initiate the blocking process when a theft is reported.[14] Other countries, such as Paraguay,

[13]CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.
[14] CITEL, PCC.I Doc. 4226p1 (XXX-17) "CCP.I/DEC. 254 (XXIX-16) – RESPUESTAS DE BRASIL" April 2017.

obligate the user to report the device directly to the operators.[15] The timeframe for compliance also varies widely between countries. Brazil mandates that all operators block a device within 72 hours of receiving a report of the IMEI filed by the user, while regulations in Paraguay dictate that operators must block them within 30 minutes.[16] Furthermore, some countries require details such as the name of the device owner and phone number associated with the device, while other countries only require the IMEI. While overlap in countries' blacklist content exists, individual countries maintain unique rules on blocking phones, which means that some phones that are blocked in one country could be legally activated by operators in another country. Finally, for reasons of practicality, most countries do not download the entire GSMA database to their local blacklist. Instead, they focus on information from neighboring countries with whom the exchange of devices is likely to be greatest, thereby reducing the regional or global effectiveness of the blacklist. However, some criminal bands move devices between distant countries and even between regions.[17] Selective exchange of information on the blacklist opens loopholes for criminals to exploit.

Additionally, device thieves have developed approaches that render blacklists less effective, such as altering the IMEIs of blacklisted devices to enable reconnection to mobile networks, or simply moving the device to a country that does not share blacklist information with the country in which it was stolen. The ability of thieves to unilaterally remove devices from a blacklist has led to consideration of other approaches in Latin America, such as whitelists.

A blacklist is only valuable if it includes accurate information on stolen, lost, or other excluded devices. If a database includes errors, such as those from inaccurate reports or human error in recording IMEIs, it can cause legitimate devices to be denied network access, and generally represents a potential single point of failure for this anti-theft approach. Further, mistakes introduced by database managers can have a domino effect when the IMEI blacklist is related to other databases, such as registers of devices that are non-homologated or have unregistered, duplicated, invalid, or unformatted IMEIs, as is the case in Colombia. Compounding the problem, errors in one country's process and database also introduce errors into, for example, the GSMA database. Due to the fact that the various databases are updated multiple times per day, ample opportunity exists for error and for one country's mistake to cause errors outside its borders.

Another potential drawback comes in the form of costs. Regardless of how a country implements its blacklist, there are costs to establish and maintain it, as well as costs to coordinate with other countries and/or a centralized database such as that maintained by the GSMA. The inclusion of information in addition to the IMEI number—such as the subscriber number and customer's personal information—can expand the size of the database, and consequently the cost associated with maintaining it. In several countries, it is the operators (and therefore, ultimately, consumers) which bear the cost for maintaining lists of blocked IMEIs and the cost of synchronizing the database(s) with the GSMA's. Notably, the cost of accessing the GSMA database varies widely depending on the type of access and status of the subscriber, but it can include a fee, a cost ultimately borne by consumers through higher service fees. Even

[15] Ministry of Public Works and Communications, Decree 6728/2017, available here. Accessed October 2017.
[16] See Paraguay, Ministry of Public Works and Communications, Decree 6728/2017, Capitulo IV, Art. 13, available here, and CITEL, PCC.I Doc. 4226p1 (XXX-17) "CCP.I/DEC. 254 (XXIX-16) – RESPUESTAS DE BRASIL" April 2017.
[17] See for example: Salinas, Lucía "Celulares y autopartes, de Colombia al mercado negro de Argentina" Clarin, May 13, 2014, available here. Accessed October 2017.

in the case of a government-maintained or subsidized database, the costs are not insignificant and require a commitment of sometimes-scarce public resources. Often, databases are maintained by a private contractor that is paid by the participating mobile operators and incorporates such costs into its service pricing.

Blacklists can be improved in order to help identify cloned and duplicated IMEIs, if information such as the SIM card number and subscriber number are also recorded, although such approaches increase the complexity of the database.

2.1.2 Whitelists

Regulators have steadily expanded the scope of IMEI blocking measures to also introduce whitelists.[18] In contrast to blacklists, which prevent devices flagged as stolen or lost from connecting to mobile networks, whitelists only list devices that have been approved to connect to such networks. The implementation of whitelists reflects a desire to address not only theft, but the trade in illicit, counterfeit, and fraudulent devices, as well as to try to complement blacklist-based solutions. In particular, whitelists are intended to address the difficulty in using blacklists to capture devices with altered or otherwise invalid IMEIs.

In order to be included in a whitelist—and thereby be authorized for connection to a network—a device must meet specific criteria, such as registration by both device importers and end users, which creates additional obligations for these two key stakeholder groups. In many cases, consumer whitelist registration takes place online,[19] but this can place a significant burden on users for whom the Internet is not easily accessible; in some cases, in-person registration is necessary. In Argentina, all devices must be associated with the personal information of the user,[20] including the user's National Identification Document (DNI). Foreign citizens, who do not have a DNI, must present their passport in person in order to verify their authenticity and have their device activated on the network.[21]

In addition to consumer registration, countries using a whitelist option require registration for all new devices that will be sold within their borders. In Peru and Colombia, for example, importers must record and report the IMEIs of all devices that will be sold within the country.[22] If these IMEIs are already included in the blacklist or whitelist, even if as a result of error or due to a fraudulent device that has appropriated the IMEI of a legitimate device that has not yet been imported into the country, then the imported devices cannot legally be sold. The requirements for information that must be registered on a whitelist vary widely between countries. For example, in Chile, importers must not only report the IMEIs of imported devices, but also the software versions installed.[23]

---

[18] In Ecuador, data from 2012 indicated that only 52% of IMEIs reported to the blacklist were being blocked, largely due to the presence of multiple devices with the same IMEI. This was cited by the regulator as part of the reason a whitelist was necessary. See CITEL, PCC.I Doc. 3655 (XVII-15) "Carpeta Tecnica: Terminales Moviles Robadas y Perdidas," September 2015.
[19] CRC, "Como Registrar tu celular?" available here. Accessed October 2017.
[20] Enacom, Resolution 8507/2016, December, 2016, available here. Accessed October 2017.
[21] Id.
[22] See Peru, Legislative Decree 1338/2017, available here, and Colombia, Ministry of Commerce, Industry, and Tourism, Decree 2025/2015, available here. Accessed October 2017.
[23] Undersecretary for Telecommunications (Subtel), Resolution 1463, Article 3, June 2016, available here. Accessed October 2017.

Unlike blacklists, there is very limited regional coordination of whitelists and data is not widely shared between countries. Each country that maintains an IMEI whitelist develops their own requirements to indicate compliance, creating an even less uniform approach than is seen with blacklists. Even if data were to be shared, the variety of standards, composition, and reporting practices for a whitelist mean that it would be extremely difficult to harmonize the whitelists of multiple countries as they stand currently. Far fewer countries maintain whitelists than blacklists; however, some regulators from countries without a whitelist have indicated that they are considering it as an option.[24] Given that mobile device theft is still an issue of concern to the public, it is likely that whitelists will continue to be implemented in the region.[25]

The implementation of a whitelist is more difficult than that of a blacklist. When compared to blacklists, whitelists are usually more costly, complicated, and cause more inconvenience to users. The implementation of a whitelist is technically difficult because in addition to new devices coming into the market, all existing legitimate devices must be added to the whitelist at the time of its implementation. This requires a concerted public awareness campaign to encourage users to register their devices. The challenge of notifying millions of consumers to register their devices led Colombia to phase in a whitelist over a four-year period, from May 2013 to July 2017.[26] Even with large awareness campaigns, disruption to consumers is inevitable.

Even without a whitelist, some countries require operators to disconnect devices that fail to meet certain conditions. For example, Argentina has begun the process of blocking phone lines that are "anonymous," meaning they do not have identifying information about the user associated with the line.[27] This approach borrows some of the aspects of a whitelist, namely that devices must meet certain conditions to connect to the network, without maintaining an actual whitelist. In the case of Argentina, the devices associated with anonymous lines are added to the national blacklist.

Whitelists can also cause unintended complications for users of legitimate devices. Colombia's Communications Regulatory Commission (CRC) notes that among other forms of altered IMEI numbers, their whitelist targets those that are duplicates of legitimate IMEI numbers. In these scenarios, both devices with the duplicated IMEI number are blocked, since there is no way to determine who is the legitimate user. This system results in innocent consumers having their IMEIs duplicated and, as a result, their device disconnected from the network. In Colombia, the issue of duplicated IMEIs is pervasive. In July 2017, the Ministry of ICT (MINTIC) estimated that 925,000 devices in Colombia have duplicated IMEIs.[28]

The high degree of accuracy necessary for a successful whitelist, combined with the low percentage of thefts that are reported to police and mobile operators in Latin America, greatly reduces the effectiveness of this type of system. Given that many thefts go unreported, it is inevitable that whitelists will contain many devices that have been stolen, but never reported. It

[24] Consultations with the regulator in Paraguay, CONATEL, indicated that the country, although not using a whitelist yet, is considering its implementation and evaluating the potential inconvenience to the users.
[25] In 2017, Osiptel, the regulator in Peru, used the fact that nearly 8 in 10 citizens feared that they would be victims of a theft of money, wallet, or mobile phone, to justify the introduction of a new whitelist policy in the country. See Legislative Decree 1338/2017, available here. Accessed October 2017.
[26] CITEL, PCC.I Doc. 4303p1 (XXX-17) CRC: "Avances del Sistema de Control de IMEI en Colombia," April, 2017.
[27] Enacom, Resolution 8507/2016, December, 2016, available here. Accessed October 2017.
[28] MINTIC, "49,6 millones de celulares fueron registrados en Colombia" July 14, 2017, available here. Accessed October 2017.

is impossible to know the scope of this problem. In addition, and while it may seem counterintuitive, there should be appropriate procedures in place for removing an IMEI from the whitelist, in the case that it was fraudulently or accidentally approved for use.

In addition, whitelists—and to some extent, blacklists—create large databases of personal information, creating a risk for unauthorized access to information. Beyond criminal attempts to access such databases, there are also risks of human error or ineffective controls protecting personal data from access by unauthorized users. In one example of the data privacy implications of these measures, the concentration of information that identifies the user of a particular device with technical information about that device, including the IMEI, could allow governments to track the likely whereabouts of a group of people at a given time based on the location of their mobile device signal.[29] The costs for developing and maintaining appropriate security protocols add to the cost and complexity of a whitelist solution, and despite best efforts, it is unlikely that any such database can be fully protected.[30]

Whitelists also place restrictions on the legal movement of devices around the region. For example, a legitimate device transported from Peru for sale in Colombia must be removed from the Peruvian whitelist as it leaves Peru, and registered on the whitelist as it enters Colombia. An approved device in one country does not automatically become approved in another country. As such, whitelists restrict the movement of devices around the region, limiting the ease with which one can connect to networks in multiple countries.

The implementation and maintenance of these lists place burdens on consumers and industry, without offering a clear benefit in return. In addition to the challenges associated with implementing and maintaining a whitelist, scant evidence exists that they actually reduce device theft. In fact, as civil society organizations have noted, such as the Karisma Foundation in Colombia, the concentration of valuable personal data within whitelists can put device users at risk of suffering from other forms of theft arising from the loss or improper treatment of that data.[31]

2.2 Technical Solutions

In comparison to the IMEI-blocking solutions mandated by governments and coordinated by operators, technical approaches to combatting mobile device theft do not rely upon blocking or approving IMEIs. Such approaches have been shown to make a significant impact on the rate of device theft. Manufacturers have taken the lead on developing and utilizing these technical solutions to curb device theft, as exhibited by the 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

[29] See Castañeda, Juan Diego, "Un Rastreador en tu Bolsillo" Karisma Foundation, July 2017, pages 24-25, available here. Accessed October 2017.
[30] In the United Kingdom, cyber-attacks exposed the data of millions of subscribers of local operators in 2016. See McGoogan, Cara, and Swinford, Steve, "Three Mobile cyber hack: six million customers' private information at risk after employee login used to access database" The Telegraph, November 18, 2016, available here. Accessed October 2017.
[31] Castañeda, Juan Diego, "Un Rastreador en tu Bolsillo" Karisma Foundation, July 2017, pages 24-25, available here. Accessed October 2017.

2015, adding another dimension to measures to combat device theft on a global scale.[32] While this initiative was widely publicized in the United States, there has been comparatively little high-profile support for technical solutions in Latin America.

The most common technical solution is an on-device anti-theft tool, often known as a kill switch, which has been shown to reduce theft rates. While the specific functionality of these features varies by device, they generally are pre-installed or available for download on smartphones, and allow the user to remotely lock a phone, erase its contents, or render the device inoperable; these functions take effect immediately. Similarly, users are able to easily and instantly reactivate a recovered device without the need for intervention by an operator or any changes to a centralized database.

Major industry players, including Apple and Samsung, were early adopters of this technology, implementing anti-theft technology in 2013 and 2014, respectively. A 2014 Report from the New York State Attorney General found that in London and San Francisco, thefts of Apple products dropped 24% in London and 38% in San Francisco in the six months after the introduction of kill switch technology.[33] In the same period, thefts of Samsung products, which did not yet have the technology as widely available, rose 3% in London and 12% in San Francisco.[34] In the year after the introduction of the kill switch on smartphones from multiple manufacturers, cell phone robberies declined 16% in New York City, 27% in San Francisco, and 38% in London.[35]

A 2015 study from Consumer Reports on mobile device theft found that in the United States smartphone thefts dropped from 3.1 million in 2013 to 2.1 million in 2014.[36] This drop corresponds with the introduction of a kill switch by many manufacturers. The findings cannot prove kill switches caused the decline, but the authors believe the decline was related at least partly to the introduction of the anti-theft technology. Broadly, these and the foregoing statistics suggest that anti-device theft technology can be a significant deterrent to device theft, with no added cost to operators, users, or governments/regulators. It is in the best interests of all stakeholders that this readily-available solution be implemented as widely as possible in order to curtail device theft.

As previously mentioned, another important feature of anti-theft technology is that it allows users to erase data on a phone. In an era where smartphones increasingly hold sensitive and important data, protecting this information can be of equal or even greater importance to the user than the fate of the device itself.

One drawback of kill switch and similar solutions is that they can only be implemented on smartphones. Accordingly, they can only deter smartphone theft. This is important because smartphones constituted about 50% of the Latin American mobile market in 2016; however, this

---

[32] CTIA, "Smartphone Anti-Theft Voluntary Commitment," April 2014, available here. Accessed October 2017.
[33] New York State Attorney General, "Secure our Smartphones," 2014, available here. Accessed October 2017.
[34] Id.
[35] 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.
[36] Consumer Reports, "Smart phone thefts rose to 3.1 million in 2013," May, 2013, available here, and "Smartphone thefts drop as kill switch usage grows," June, 2015, available here. Accessed October 2017.

is expected to rise to 70% by 2020.[37] Additionally, in some countries smartphones make up the vast majority of mobile phone sales. For example, in Brazil in 2016, 9 out of every 10 mobile phones sold were smartphones.[38] Furthermore, the vast majority of these smartphones are sold with preinstalled anti-theft technology, or are capable of downloading it.[39] As smartphone penetration in Latin America continues to rapidly increase, the majority of mobile devices in the region will contain theft-deterring technologies. These trends call for careful stakeholder consideration of how best to use all available tools to deter device theft.

A second drawback of kill switch technologies is that they require users to activate the service, or opt-in, before a device is stolen or lost. Such an approach is required because the owner of a new device must go through the process of registering or otherwise linking the device to the anti-theft service in order to enable the use of a different device (such as a PC or a friend's mobile device) to remotely locate or disable the lost or stolen device, or to erase its data. If a mobile device is stolen or lost before the user activates the anti-theft service, they are unable to remotely disable or wipe their device. However, a thief has no way of determining in advance whether a user has opted into the kill switch service, making all smartphones that have kill switch technology available equally unattractive.

Although the majority of press coverage and research related to kill switch solutions focuses on the United States and United Kingdom, the functionality is available to smartphone users worldwide by virtue of being enabled with a downloadable application. In Latin America, however, there has been little consumer education regarding the available tools by operators, governments, or regulators.

Table 1: Comparison of Available Solutions

	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

[37] GSMA, "The Mobile Economy Latin America and the Caribbean 2016" 2017, available here. Accessed October 2017.
[38] Counterpoint Research "Despite Recession, Brazil LTE Smartphones Grew 53% Annually in 2016" March 3, 2017, available here. Accessed October 2017.
[39] In the first quarter of 2017, Android and iOS devices, both of which are anti-theft technology enabled, made up 99.7% of the global smartphone market. See International Data Corporation "Smartphone OS Market Share, 2017 Q1," available here. Accessed October 2017.

	Pros	Cons
		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.
Kill Switch	• 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.

2.3 Role of Law Enforcement

In addition to IMEI-blocking and technology-based solutions, law enforcement agencies are critical participants in the fight against device theft. Ideally, law enforcement would be empowered to focus on the aspects of device theft that enable it to proliferate on a large scale, such as the systematic modification of the IMEIs of stolen devices and the entry of illicit devices into a country. However, the current approaches in Latin America have not significantly reduced theft, as discussed in Section 3.5 – Effectiveness of the Current Approach, creating a situation in which law enforcement must commit resources to receiving device theft reports and attempt to track down stolen devices.

While theft is a crime in the countries where mobile device theft is an issue, not all of the actions that are part of the stolen device life cycle are equally prioritized by law enforcement. This is especially true for cloning or modifying the IMEI numbers of devices, a key part of the criminal enterprise in stolen devices that in many countries has only recently been criminalized.[40] The activities that allow stolen devices to re-enter the marketplace, and often to appear legitimate, need to be as vigorously addressed by law enforcement as the actual theft itself. Partnerships with law enforcement to help combat the black market in stolen devices is essential. In Ecuador, information gathered in the process of blocking devices concerning suspected locations where stolen devices are being sold is shared with law enforcement.[41] Law enforcement in Buenos Aires have also been able to use this technique to identify stores selling stolen devices.[42] This kind of cooperation that uses existing information from operators to track down illegal activity is an example of the positive role law enforcement can play.

While law enforcement plays a key role in supporting a solution to mobile device theft, in some cases they inadvertently undermine efforts to combat theft. In the Dominican Republic, the law requires users to notify their operators of a stolen device.[43] However, the police often advise consumers not to do so, with the hope that they can use the signal of the device to track its location.[44] Such mixed messages undermine the success of the entire anti-theft approach. In order to be successful, law enforcement, regulators, and operators must work in concert.

Greater implementation of technology-based solutions would change the role of law enforcement agencies with respect to device theft and makes individual users active participants in efforts to protect their own devices and data. Options such as kill switches empower users to locate and, if appropriate, wipe and deactivate their devices, freeing law enforcement resources from the obligation to investigate individual device thefts. Based on data available from the United States and United Kingdom, kill switch approaches have reduced device theft overall, allowing law enforcement to spend more time and resources combatting larger players in the stolen devices ecosystem, including those that alter devices and transport and sell illicit devices in large quantities.

---

[40] See for example, Honduras, where the Senate approved measures to sanction the modification of IMEIs in August 2017. Congreso Nacional "Congreso Nacional aprueba decreto que sanciona fuertemente a quienes clonen IMEI de teléfonos celulares," available here. Accessed October 2017.
[41] CITEL, PCC.I Doc. 3655 (XVII-15) "Carpeta Tecnica: Terminales Moviles Robadas y Perdidas," September 2015.
[42] See: Via Buenos Aires, "La Policia busca a los dueños de 2.500 celulares que fueron recuperados," May 12, 2017, available here. Accessed October 2017.
[43] CITEL, PCC.I Doc. 4226p2 (XXX-17) "Informe sobre la consulta de los procesos de intercambio y bloqueo entre países de los IMEI de dispositivos móviles con reporte de hurto o extravío," April, 2017.
[44] Id.

Section 3. Existing Initiatives in Latin America

3 Existing Initiatives in Latin America

3.1 Regional Initiatives

Mobile device theft is an intrinsically transnational issue as stolen phones can be moved easily across borders to avoid detection, often being connected to organized crime.[45] As Latin American governments have recognized, this type of cross-border crime requires regional initiatives. In 2011, and initiated by the Colombian government, CITEL approved a Resolution to invite member states to 'adopt, strengthen, or complement the measures needed to minimize the theft of mobile terminal devices and their activation and marketing at the regional level.'[46] This was a starting point for increasing regional action and cooperation on the issue. This Resolution prompted CITEL to form a Rapporteurship on Fraud Control, Regulatory Non-Compliance Practices in Telecommunications and Regional Measures Against the Theft of Mobile Terminal Device within the Permanent Consultative Committee I: Telecommunications / Information and Communication Technologies (PCC.I) to focus on these issues. Following actions by the rapporteurship, PCC.I has asked member states to contribute updates on measures they are taking to address of fraud and handset theft. The most notable action is a technical workbook compiling such measures, PCC.I Doc. 3655/15 rev.1 (XXVII-15), last updated in 2015.[47] The rapporteurship has also held workshops to address device theft issues, most recently in March 2016. The group advocated for a seminar on counterfeit and stolen devices, which was approved in April 2017 and will take place in conjunction with the next PCC.I meeting, scheduled for March 2018.[48]

The GSMA has also been very proactive in developing a regional response to this issue and has been successful in advocating for operators to exchange their blacklist data. With 77% of the operators in the region connected to the GSMA's blacklist in some form, it represents one of the most comprehensive regional responses to device theft.[49]

In April 2013, the Andean Community of Nations (CAN), formed by Bolivia, Colombia, Ecuador and Peru, released Decision 786, "Information exchange of mobile terminal equipment lost, stolen, or stolen and recovered in the Andean Community," with the aim of creating a legal framework on device theft between mobile operators in the Andean Community.[50] Its decisions are binding for its members and must be implemented into law by each country. According to Decision 786, mobile providers must: (i) exchange information related to mobile terminal devices lost, stolen, or stolen and recovered in the Andean community; (ii) block mobile terminal

[45] El Comercio, "Las mafias movilizan los celulares robados entre los países de la Región," 2014, available here.
[46] CITEL, PCC.I/RES. 189 (XIX-11) "Regional Measures to Combat the Theft of Mobile Terminal Devices," September, 2011, available here. Accessed October 2017.
[47] Creation of the technical notebook was approved by CITEL, PCC.I/RES. 217 (XXIII-13) "Technical Notebook on Stolen, Robbed and/or Lost Mobile Terminals," available here. Accessed October 2017.
[48] CITEL, PCC.I/RES. 280 (XXX-17) "Seminar on Control of Mobile Devices with Altered/ Duplicate Identifiers," May 2017, available here. Accessed October 2017.
[49] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.
[50] Official Gazette No. 2186, "Decision 786: Intercambio de información de equipos de terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina," April 26, 2013, available here. Accessed October 2017.

devices reported as lost or stolen; (iii) use the GSMA IMEI database; and (iv) develop information and campaigns aimed at mobile users on the importance and need to report the loss or theft of mobile devices to providers and appropriate authorities.[51]

The Telecommunications Regional Technical Commission (COMTELCA) is a Central American governmental organization that coordinates and harmonizes the regional development of the telecommunications industry. Its member states are Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Nicaragua, and Panama. All mobile providers in these countries have cooperation agreements with the GSMA to exchange their blacklist information, however to date, some operators still have not connected to the GSMA database.[52]

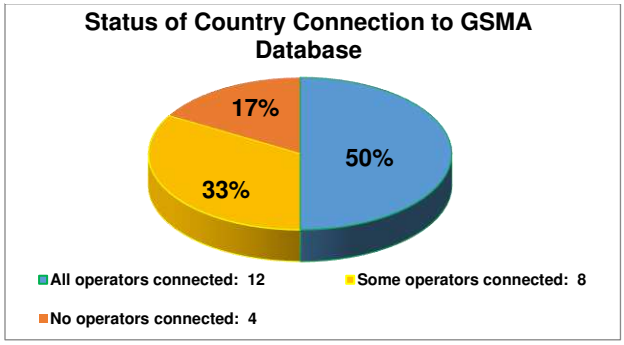
Regional coordination has been an important factor in facilitating the approval of measures to address theft across multiple countries. The measures promoted by regional bodies also offer a roadmap to new countries looking to adopt additional measures to combat mobile device theft. However, it is important to note that actual policy has been formed at the national level, resulting in a multitude of systems that are different in form and function across the region. The lack of consistency reduces the effectiveness of the overall system and increases costs, especially when devices move across borders and must comply with multiple distinct regulatory regimes.

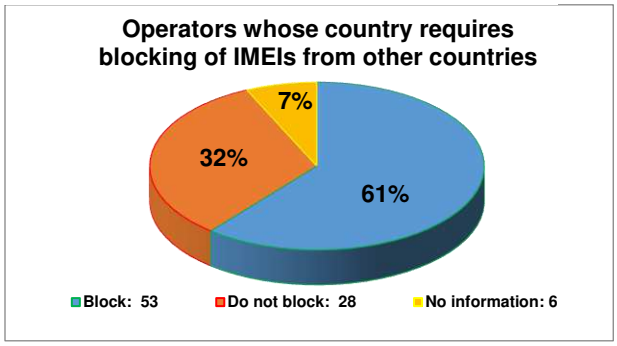
3.2 Blacklist and Whitelist Policies

The majority of Latin American countries have taken some form of action to combat device theft. As of March 2017, 64 out of 87 operators in the Americas were connected to GSMA's IMEI database and an additional three operators were in a testing phase, with plans to fully connect to the database.[53] As shown in Figure 3, a vast majority of operators around the region subscribe to the blacklist, but as noted earlier, not all of them make use of the database in the same manner.

[51] Official Gazette No. 2186, "Decision 786: Intercambio de información de equipos de terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina," April 26, 2013, available here. Accessed October 2017.
[52] See COMTELCA presentation "Joint Online ITU-CITEL Workshop on Global Strategies against Mobile Device Theft," slide 12, March 16, 2016, available here. Accessed October 2017. Also, for current status of operator connections to GSMA database, see CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.
[53] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.

Figure 3: Status of the operators' connections to the GSMA database





Source: GSMA[54]

Despite the widespread subscription to the GSMA database, each country maintains their own processes for blocking devices and rules for exchanging blacklist information, which limits a harmonized regional policy. As Figure 3 shows with respect to requirements to block blacklisted IMEIs from other countries, there are 28 operators (or 32% of those surveyed) for which their country of operation does not require them to block IMEIs blacklisted in other countries, although in some cases, such as the Dominican Republic, each operator sets their own policy regarding use of the GSMA blacklist.[55] This non-participation in the shared database represents a weakness of the blacklist system, creating a pool of operators that are more likely to allow activation of a stolen device because IMEIs are not checked against other countries' blacklists.

3.3 Technological Solutions

In contrast to blacklist- and whitelist-based efforts, there has been comparatively little emphasis on technological solutions by Latin American governments. A 2015 publication by the Colombian Communications Regulatory Commission surveyed 20 countries in the Americas regarding their efforts with manufacturers to reduce mobile device theft, including the use of kill switches.[56] Of the 12 countries that responded, 73% had taken no such action, and only the United States was actively managing initiatives related to kill switches.

Despite relatively little promotion from key stakeholders (e.g., governments and operators), kill switch technology has been addressed in the mainstream media from time to time. For

[54] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" July 2017.
[55] CITEL, PCC.I Doc. 4226p2 (XXX-17) "Informe sobre la consulta de los procesos de intercambio y bloqueo entre países de los IMEI de dispositivos móviles con reporte de hurto o extravío," April, 2017.
[56] CRC, "Fortalecimiento de las bases de datos dentro de la estrategia nacional contra el hurto de equipos terminales móviles. Documento soporte propuesta" page 31, August 2015, available here. Accessed October 2017.

example, a popular Argentine newspaper reported on kill switch offerings for devices employing operating systems from Apple, Google, Microsoft, and BlackBerry.[57]

3.4 Current Policies by Country

Perhaps the most important component to understand regarding national approaches to device theft in Latin America is that each country takes a slightly different approach. While certainly intended to address what policymakers and regulators view as solutions tailored to their country's needs, the result is a patchwork of policies and approaches that creates difficulties with respect to harmonization and data sharing.

For example, Peru not only requires that new devices be registered on the national whitelist, but that each device be associated with a corresponding entry of the device user in the national civil registry.[58] This dramatically increases the level of accuracy necessary for the correct function of the whitelist and imposes significant burdens on the consumer. Any errors in either the whitelist or civil registry databases can easily result in a situation where consumers are unable to use their phones. Each citizen is also limited to a certain number of devices purchased abroad within a calendar year. These strict requirements and limits on foreign devices can make it more difficult to change devices.

This approach is not limited to Peru. Although Argentina has not implemented a whitelist, the National Communications Entity (Enacom) is in the process of requiring every device to be connected to the national identity number of its owner.[59] Users found to have excessive numbers of IMEIs registered will be considered for blocking from the network. These policies make the free flow of devices very difficult, and increase the inconvenience for consumers travelling with their devices across borders. Additionally, this makes it more difficult to switch SIM cards between devices.

Table *2* shows an overview of the policies and associated implications for consumers, operators, and manufacturers in several countries throughout the region. The information presented, although not exhaustive, is designed to show the diversity of approaches throughout the region, and some of the implications that these policies can have for operators, consumers, and governments. Wherever possible, relevant resolutions are cited, though it should be noted that some regulations are not listed here and that some device theft measures are authorized by agreements with the GSMA or private operators, not by a government regulation or law. The table below is intended to provide the reader with a guide to the general legal framework regulating policy in each country.

[57] La Nación, "Cómo proteger tus equipos electrónicos con un software de monitoreo," February 24, 2015, available here. Accessed October 2017.
[58] Legislative Decree 1338/2017, available here. Accessed October 2017.
[59] See Enacom, Resolution 2459, available here. Accessed October 2017.

Table 2: Overview of policies by country

	Blacklist					Whitelist			
Country	**Blacklist Implemented**	**Consumer Obligations**	**Operator Obligations**	**Manufacturer / Import Export Obligations**	**Law enforcement Access**	**Whitelist Implemented**	**Consumer Obligations**	**Operator Obligations**	**Manufacturer / Import Export obligations**
Argentina	Yes, see Resolution 2459/2016.	Register personal details with operator, with lines per person capped at 5. Also report theft or loss of device.	Share data with other operators and with the GSMA database.	SIM cards not registered with personal details of user cannot be activated on the network.	Judicial authority has access to blacklist.	Under consideration.	N/A	N/A	N/A
Brazil	Yes, see General Telecommunications Law and Resolution 477/2007	Users must report thefts to operator or police in order for the blocking process to begin.	Block devices within 72 hours, and synch with GSMA database. Operators pay to maintain blacklist.	No	Police can initiate report to block device.	No	N/A	N/A	N/A
Chile	Yes, see Decree 157/2011.	Users must report thefts in order for the blocking process to begin.	Block reported IMEIs, maintain 24/7 line for reporting stolen devices, record personal details, telephone number, time and date of theft, whether the theft has been reported to law enforcement, of all reported devices, share reported information with the Portability Management authority (OAP).	No	The OAP maintains details of each device reported stolen or lost. The police have access to this list.	Yes, for purposes of homologation, especially for imported devices. Regulator is internally considering additional whitelist measures, but has not made a timetable public. See Resolution 1463/2016.	Users who import devices for personal use must have the device certified as compliant.	Add existing devices in use in country to whitelist, only allow homologated devices to be activated on network, maintain list of certified devices.	Devices must be certified as homologated prior to sale in the country and labelled as appropriately certified.

	Blacklist					Whitelist			
Colombia	Yes, see Law 1453/2011, and Decree 1630/2011[60]	Users must report stolen and lost devices in order for the blocking process to begin.	Block devices with reported IMEIs and devices with altered/improper IMEIs. Assume costs of maintaining database. Maintain channels for users to report stolen and lost devices. Share data between operators and with GSMA.	Register imported devices on whitelist.	Police and Prosecutors have access to both white and blacklist.	Yes, see blacklist column and also Decree 2025/2015.	Register existing devices on whitelist or face disconnection from network.	Monitor networks, block unauthorized devices. Only allow homologated, registered devices access to network. Maintain lists of personal details of users associated with each device. Block devices with duplicated IMEIs.	Register imported devices before sale.
Costa Rica	Yes, see Telecommunications User Protection Regulation.	Users must report thefts in order for the blocking process to begin.	Block the device with reported IMEI from connection to network, share database with other operators. All operators exchange information with the GSMA blacklist.	No	No	No	N//A	N/A	N/A
Dominican Republic	Yes, see Resolution 137-09.	Obligated to report stolen and lost devices.	Block reported devices, report IMEIs to national blacklist. Operators also share information with GSMA database.	Devices must be checked against the national blacklist before they can connect to the network.	Recommend to avoid blocking device with goal of tracking stolen devices.	No	N/A	N/A	N/A

[60] Also see CRC Resolution 3128/2011 (modified by CRC Resolution 4868/2016) and CRC Resolution 4813/2015.

	Blacklist					Whitelist			
Ecuador	Yes, see Resolution No. 191-07-CONATEL-2009 (and subsequent modifications in Resolutions TEL 214-05-CONATEL and TEL 535-18-CONATEL).	Users must report thefts in order for the blocking process to begin.	Block devices with reported IMEI, share information with other operators and government run blacklist. Operators also exchange information with the GSMA.	Blacklisted devices or devices that share an IMEI with a device of the backlist cannot be connected to the network.	Attorney General is notified of reports of businesses and markets where stolen phones are sold.	Yes, see resolutions cited for blacklist and Resolution 111-2013.	Register existing devices on whitelist.	Monitor networks and block unauthorized devices, including those with duplicated IMEIs.	Register imported devices on whitelist.
Honduras	Yes, see Resolution NR009/14.	Users must report thefts to operators for the blocking process to begin. In order to unblock a recovered device, users must physically present themselves at the offices of the operator.	Operators must pay to maintain blacklist, exchange information with GSMA daily, block phones on blacklist from connecting to network. Operators must also maintain information about the consumer associated with every device in order to facilitate the blocking process when a stolen device is reported. Operators must maintain a phone number available 24/7 with a response time of 20 seconds to accept reports of phones to be blocked.	Devices imported from abroad cannot connect to the network if the IMEI is present on the blacklist.	Any "competent judicial or administrative authority" will have access to the national registry of devices in the country.	Approved[61] August 2017, will be implemented in 2018.	SIM cards and IMEI numbers must be registered by user in order for device to connect to network, including individuals who bring a device into the country from abroad.	Operators will monitor networks and cannot connect devices to the network unless they are included in the whitelist, and must maintain personal details of the user of all devices.	Imported devices will have to be registered on the whitelist prior to connecting to the network.

[61] At time of publication, the reforms to Decree 19-2014 had been approved, but not yet officially published.

	Blacklist					Whitelist			
Mexico	Yes, see Federal Telecommunications and Broadcasting Law (2014) and Technical Provision IFT-011-2017.	In order for the blocking process to begin, users must report stolen devices.	Block reported IMEIs immediately, allow users to consult status of IMEI, prevent connection to network of duplicated IMEIs, or of devices reported as stolen or lost.	Devices with an IMEI in the blacklist cannot receive a certificate of homologation.	No	No	N/A	N/A	N/A
Paraguay	Yes, see Decree 6728/17.	Users must report stolen and lost devices.	Block reported devices within 30 minutes, keep record of most recent 3 IMEIs associated with every phone line. Share information with other operators and GSMA.	No	Police and Attorney General have access to database.	Under consideration.	N/A	N/A	N/A
Peru	Yes, see Resolution 138/2012 and Legislative Decree 1338/2017.	Users must report stolen, lost, and inoperative devices.	Block reported devices from connecting to the network, share data on reported devices with government administrators of database. Block devices at request of government.	See whitelist obligations for importers/exporters.	Police can request access to database in course of investigations.	Yes, see resolutions cited in blacklist column.	Register personal details of user associated with each device, block unauthorized devices from connecting to the network, including all duplicated IMEIs.	Block all devices not on whitelist.	Imported devices must be added to the whitelist before being sold. Exported devices must also be reported to ensure they are removed from the whitelist.

Source: TMG research

3.5 Effectiveness of the Current Approach

A blacklist's success depends on robust and accurate reporting practices, which are difficult to achieve in regions where the majority of crimes often go unreported. In Colombia, for example, only an estimated 4% of phone thefts were reported to the police in the first half of 2017.[62] In Brazil, a recent survey found that only 51% of victims of cell phone theft notified the police.[63]

Thefts have stabilized as thieves have discovered workarounds to the blacklist system, especially by tampering with IMEIs. In fact, in August 2017, the Attorney General of Colombia asked the government to come up with a new strategy to address phone theft, saying that the current IMEI blocking strategy had failed.[64] A study of mobile device theft in Colombia showed that the number of thefts in 2016 was 46.7% higher than in 2010, although there was a slight decrease between 2015 and 2016.[65] The Attorney General's Office also notes that mobile phone theft is the fastest growing form of crime in the country, increasing 79% from the first six months of 2016 to the first half of 2017. This increase occurred despite the imposition of specific anti-theft regulation (focused on IMEI blocking) in 2011.

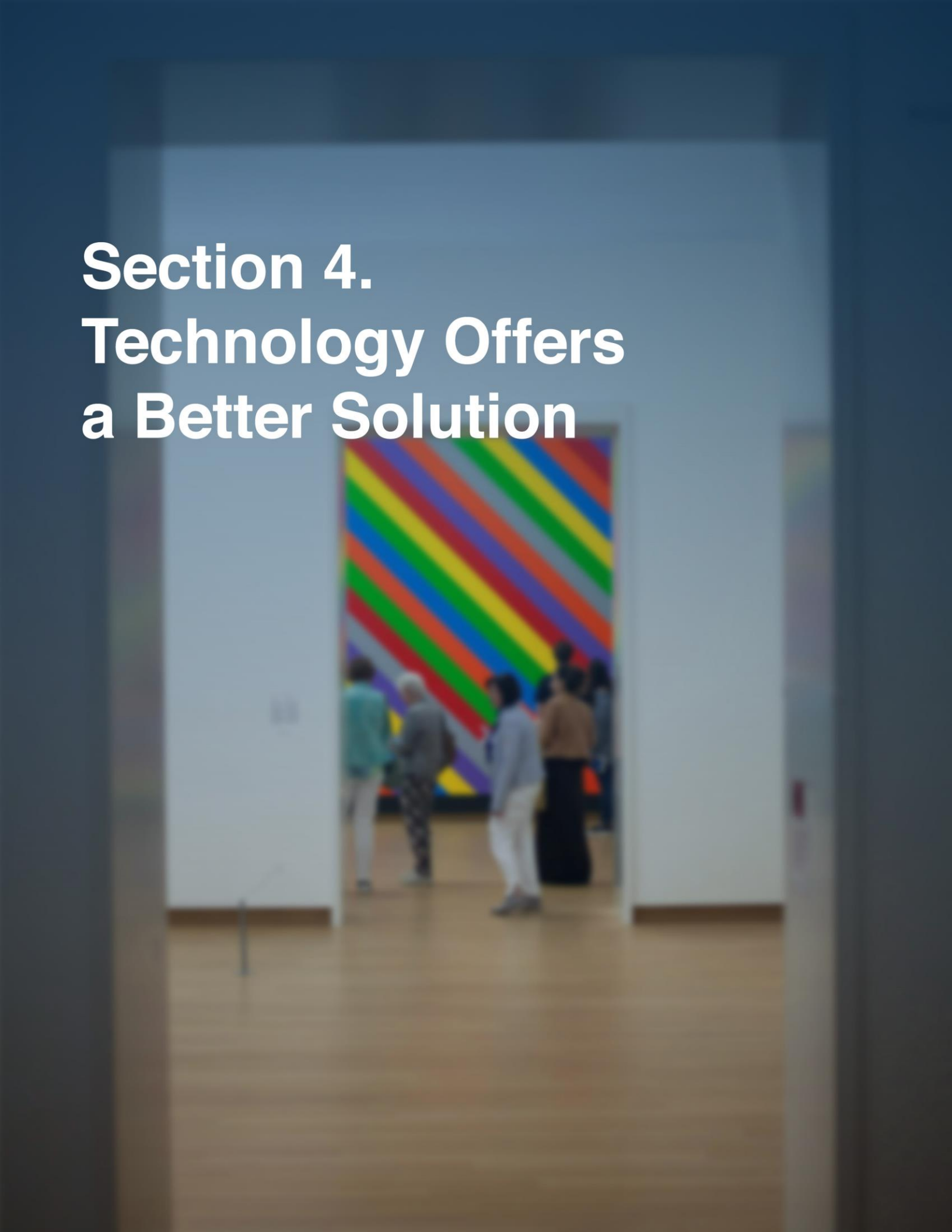
While Brazil created a national database of stolen devices in 2000 which was subsequently connected with the GSMA database in 2014, theft levels have not significantly decreased. In fact, In Rio de Janeiro, data released by the Public Security Institute for July 2017 showed a 47.1% increase in cellular device thefts compared to the same month a year prior.[66] While comprehensive data on levels of mobile device theft are not always readily available, reports such as this indicate that mobile device theft is still a significant problem in Latin America and that IMEI blocking measures inadequately addressed the issue.

In the years since their introduction, IMEI-based approaches have been leveraged to address problems well beyond their original scope, which was to reduce the incentive for mobile phone theft. For example, issues such as the use of fraudulent IMEIs and the market for stolen handset components cannot easily be addressed by IMEI-based measures and will require new and innovative tactics.

---

[62] El Tiempo, "Colombia es el país de la región con mayor robo de celulares," August 8, 2017, available here. Accessed October 2017.
[63] Panorama Mobile Time/Opinion Box, "Roubo de celulares no Brasil," July 2017. Available for download here. Accessed October 2017.
[64] Attorney General, "Press Release: El bloqueo de los Imei de los celulares no está funcionando," August 4, 2017, available here. Accessed October 2017.
[65] Claudia Rodriguez, Juan Sebastian Moreno and Juan Felipe Godoy (Universidad de los Andes), "Informe seguridad 2016," July 2017, p. 6, available here. Accessed October 2017.
[66] Instituto de Seguranca Publica, "Comparativo das Incidências Publicadas No Diário Oficial Do Estado Do Rio De Janeiro," August 24, 2017, available here. Accessed October 2017.

Section 4. Technology Offers a Better Solution



4 Technology Offers a Better Solution

It is widely accepted, even by the GSMA itself, that blocking devices based on IMEI numbers is unlikely to be effective as a solution on its own.[67] And as noted above, neither blacklists nor whitelists, even when used jointly, resolve the issue of device theft, and both involve costs borne by some combination of regulators, operators, and users. Given these limitations, Latin America would be best served by an approach that increases the visibility and use of technology-based solutions, complemented by blacklists, as well as an updated legal system that criminalizes key activities involved in the collection, modification, and dissemination of stolen devices.

4.1 Benefits to Latin America

As noted in Section 2.2 – Technical Solutions and Section 2.3 – Role of Law Enforcement, technological solutions to device theft bring significant benefits that cannot be achieved by IMEI-blocking approaches, particularly when compared to whitelists:

- **Successful.** Most importantly, kill switch solutions have been shown to reduce smartphone theft, unlike the blacklist and whitelist solutions favored by many Latin American governments. A solution with measurable success should be promoted by all stakeholders.
- **No cost to governments, operators, or consumers.** Technological solutions to date are enabled by manufacturers and users, with no investment in resources or time required to create or maintain a database, for example, or to create mechanisms for cross-border coordination.
- **Refocus law enforcement resources.** As noted in 2.3, technological solutions allow law enforcement to better focus resources on the underlying problems and responsible parties, reducing the time required to record device theft reports and track down individual devices.
- **Industry-led, user-controlled solution.** Technological solutions can be implemented without the need for new regulations or laws. Instead, manufacturers develop approaches that are controlled by users, and ease of use or new functionality can even be a point of differentiation and competition between manufacturers. Such an approach should avoid the addition of new complexity to the legal and regulatory framework.
- **Available today.** Major manufacturers and operating system providers, including the Android and iOS ecosystems, already offer technological solutions to make device theft less lucrative. This is not a future technology, but one that can be readily activated today. As smartphone adoption increases, a greater percentage of devices in circulation will include kill switch technology. This is in marked contrast to list based approaches, which can take years to fully implement.[68]

---

[67] 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, and CITEL, PCC.I Doc 4303p1 (XXX-17) "Avances del Sistema de Control de IMEI en Colombia" slide 9, April 2017.

[68] Colombia's whitelist was phased in over a period of four years from May 2013 to July 2017. See CITEL, PCC.I Doc 4303p1 (XXX-17) "Avances del Sistema de Control de IMEI en Colombia" slide 5, April 2017.

- **Anti-theft as a smartphone selling point.** The inclusion or easy availability of technological anti-theft solutions could potentially be an attractive characteristic of smartphones, making informed consumers more likely to purchase and use a smartphone, a goal in line with preferences of operators and other stakeholders.
- **Easily reversible.** In the event that a stolen or lost device is recovered, users can easily unblock the device without having to file a new report with their operator. This is a simpler process that frees up resources of operators and the government to focus on other priorities and could help lower maintenance costs associated with list-based approaches.

4.2 Improved Blacklists to Complement Technology

While technological solutions will be a crucial tool for reducing device theft, improved usage of blacklists does hold promise as a complementary solution. Blacklists can help make sure that stolen devices cannot reconnect to networks, and can be used with all types of devices that can connect to a mobile network, including feature phones.

However, there are important ways in which blacklist implementation and usage can be revised in order to improve effectiveness:

- **Greater harmonization and adoption.** A major weakness of blacklists is the lack of harmonization and uniform adoption. Blacklists would be more effective if all participants, even across national borders, used a uniform approach that simplified information sharing, thereby also reducing costs.
- **Global reach.** A blacklist is only as helpful as it is widespread. Increased global adoption would eliminate the markets in which stolen devices are most likely to be sold, reducing demand for such devices. A regional approach does not deter the movement of stolen devices to a different region where they will not appear on a blacklist.
- **Improved data accuracy.** Blacklists are also only as effective as the accuracy of the data they contain. Operators and database managers must redouble efforts to ensure the inclusion of accurate IMEI information in order to only target legitimately stolen devices.

It is important to note, however, that improved blacklists will be most effective when used as one component of a holistic approach that builds upon the success of technological solutions and 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.

Ultimately, however, policymakers must evaluate the importance of investing in blacklists as the market shifts to smartphones capable of technological solutions. Committing resources to blacklists is an investment in an approach that will become less relevant as the market continues its evolution. Regulators should begin to consider whether money currently invested in list-based approaches could be better spent in other ways, for example, by helping to promote and educate the public on technology-based anti-theft tools.

4.3 Consumer Education

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. The anti-theft technology on smartphones is often available on an opt-in basis, making consumer education critical to most effectively leveraging anti-theft

technologies. If users are unaware of a feature or how to properly use it, then its effectiveness is undermined. Furthermore, policies to make reporting the IMEI of a stolen device less burdensome can help improve the effectiveness of measures to counter device theft.

In Latin America, initiatives to address device theft are not as common, especially on a regional level. However, the GSMA has been active in consumer awareness initiatives, especially with the "We Care Campaign," a joint campaign between the GSMA and mobile providers around the region.[69] The campaign includes measures to make it easier for consumers to check the status of an IMEI in real time. This mechanism, called the IMEI device check, allows users to check the history of the IMEI of a device that they own or are considering purchasing against the GSMA blacklist.[70] Since its inception in 2014, the campaign has had 13 launches around the region and 18 public announcements of industry initiatives.[71] This campaign empowers users to make informed decisions when purchasing new devices and allows them to play a constructive role in the fight against device theft.

Latin American consumer education initiatives, such as the GSMA campaign, have tended to focus more on IMEI registration and reporting, not on how to leverage the benefits of anti-theft technology. This is not to say that these initiatives cannot play a constructive role. In the case of blacklists and whitelists, the database is far more reliable and useful when the IMEIs of stolen devices are reported, and when users are empowered to check the status of devices they own or are considering purchasing, both of which rely on consumer education in order to reach their full potential. Brazil implemented a website in which consumers can verify the status of a specific IMEI, especially before making a purchase.[72] Web-based portals run by either regulators or operators where users can check the status of their IMEI are widespread throughout the region.[73] In countries where existing devices in the market are scheduled to be disconnected from networks unless the consumer takes certain remedial action, such as registering the device, sending text messages directly to users to inform them of their obligations is also a common tactic.[74] These measures send information directly to those who are affected, instead of less targeted campaigns like print or television advertising.

However, these Latin American initiatives do not address the role a technical solution can play in preventing device theft, as mentioned in 3.3. Strategies to prevent device theft could be greatly enhanced by widespread awareness of the security advantages of smartphones. If users are aware that a device with anti-theft technology is readily available in their market and can deter theft, then the incentive to purchase a smartphone increases.

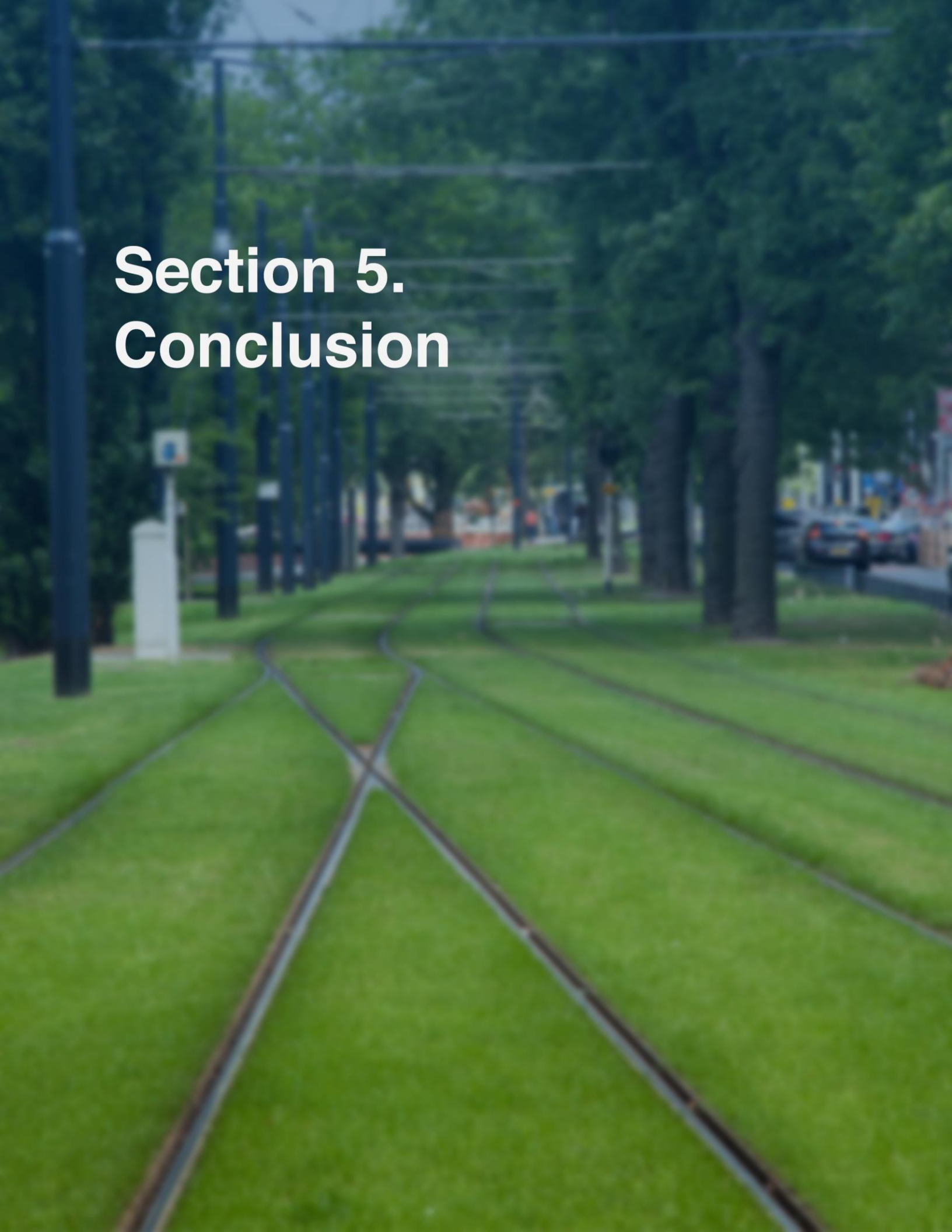
Opportunities exist to greatly improve measures to counter mobile device theft in Latin America by promoting the benefits of anti-theft technology and educating consumers on the benefits of smartphones that are enabled with this technology. In the United States, efforts by the attorneys general in New York and San Francisco, as well as legislation in Minnesota and California

---

[69] GSMA, "We Care Campaign" official website, available here. Accessed October 2017.
[70] GSMA, "GSMA Device Check" official website, available here. Accessed October 2017.
[71] GSMA, "We Care Campaign" official website, available here. Accessed October 2017.
[72] Portal Brasil, "Anatel aprimora regras para coibir roubos e furtos de celulares," March 9, 2016, available here.
[73] See for example: Enacom, "Consulta de IMEI," available here; Entel, "Quieres saber si tu equipo está bloqueado" available here; CRC, "Como registrar tu celular," available here. Accessed October 2017.
[74] Brazil is currently moving forward with such a program, although there is not yet a fixed date for disconnection of devices. See: Anatel, "Press release- BLOQUEIO DE CELULARES IRREGULARES," July 17, 2017, available here. Accessed October 2017.

prompted widespread media coverage of the issue of device theft, and helped promote awareness of the potential benefits of technology-driven anti-theft tools.[75] This was complemented by the public commitment of CTIA member manufacturers to address the issue, which brought additional visibility to the issue. Such approaches on behalf of both government and industry could serve as models to be employed in Latin America in order to raise awareness of technological anti-theft solutions.

[75] See for example: Martyn Williams "10 things to know about the smartphone kill switch," PC World, June 24, 2014, available here, or Hayley Tsukayama, "The smartphone 'kill switch,' explained," The Washington Post, August 27, 2014, available here. Accessed October 2017.



Section 5. Conclusion

5 Conclusion

Policies have been adopted in various Latin American countries to address mobile device theft. In particular, blacklists of stolen devices have been widely adopted throughout the region. However, their effectiveness has been mitigated by weaknesses in the blacklist approach and a lack of uniformity and harmonization. Additionally, criminals have thwarted such policies by successfully exploiting weaknesses and developing countermeasures.

Subsequently, blacklists have been supplemented by other IMEI-based approaches, such as whitelists, in order to improve the effectiveness of efforts to counter device theft. Whitelists emphasize policies that address device theft as one of several related problems, including counterfeit and fraudulent devices. However, whitelists also have several drawbacks that undermine their effectiveness, particularly because they still lack regional harmonization and inconvenience both consumers and industry.

Despite the implementation of both blacklists and whitelists, device theft remains a serious problem in Latin America. Although Latin American governments have strongly supported blacklists and other IMEI-based blocking tools, there has been little public discussion of technological anti-theft solutions that can prove to be more effective, less costly, and require less government involvement. Approaches such as the kill switch technology that major manufacturers have implemented can make device theft less lucrative without requiring a commitment of additional public funds or other resources, or imposing costly burdens on consumers and businesses. Complemented by improved blacklists and consumer education initiatives to inform customers how to make use of the anti-theft measures available to them, technological solutions have significant potential to reduce mobile device theft in Latin America. Further, the implementation of a technological solution has the added benefits of allowing law enforcement to focus their efforts on the underlying criminal elements and behaviors that enable device theft, as well as possibly encouraging greater smartphone adoption.