CROG#9 Doc 00X

Common position proposal on signal inhibitors (jammers) in Latin America

Meeting Information	
Meeting Name and Number	CROG#9
Meeting Date	26 February 2014
Meeting Location	Barcelona, Spain
Document Information	
Document Author	José Antonio Aranda, GSMA Alexis Arancibia, GSMA
Additional Contributors	Andrea Espinoza Lechuga, América Móvil Héctor Huerta Reyna, América Móvil José Gilberto Fragoso Gómez, América Móvil
Document Creation Date	3 March 2014
Document Status	Approval
Security Classification	Confidential to CROG Latam Member
Document Summary	
This document contains a common position proposal on signal inhibitors (jammers) in Latin America presented for discussion within CROG Latam.	

Version History (to be completed by editor)		
Date	Version	Author / Comments
3 March 2014	0.1	José Antonio Aranda, GSMA and América Móvil México
19 March 2014	0.2	Brenda Mana, GSMA
27 March 2014	0.3	Alexis Arancibia, Adrian Dodd, Sandy Gomo, GSMA
28 March 2014	0.4	Adrean Rothkopf, Millicom and Team Honduras/Colombia
8 April 2014	0.5	Alberto Boaventura, Oi Brazil
9 April 2014	0.6	SEGF Review: Ana Marcela Arévalo, Telefónica Colombia; Leonel Alejandro Aquino, Movistar Costa Rica; Diego Bassanelli, Telecom Argentina, Luis Becerra, Antel Uruguay
29 April 2014	0.7	SEGF Review2: Mercedes Aramendía, Telefónica Uruguay; Leonardo Saunero Nuevatel Bolivia; Nelson Enrique Bermúdez, Tigo Colombia
16 May 20014	0.8	Andrea Espinoza Lechuga, América Móvil; José Montes de Peralta, Nextel Perú; Bernardo Cabrera, Roberto Riela, Telefónica Uruguay.
16 Jun 2014	0.9	REGU Review: Juan Patricio Cristi Orellana, Entel Chile; Yamil Habib, Telefónica México; Zulmari Artigas, Telefónica Venezolana; Mercedes Aramendia, Telefónica Uruguay: Andrea Espinoza Lechuga Rev1, América Móvil; Antonio Díaz Hernández, Nextel México, Daniela Cuellar, Millicom; Acisclo Valledares, Tigo Guatemala; Nelson Bermúdez, Tigo Colombia; María Teresa Orellana de Rendon, Tigo El Salvador; Pedro Solares C., Novatel Bolivia; Rafael, Antel Uruguay; Francisco Evertsz, Telefónica Guatemala, André Aprigio, TIM Brasil, Francisco Javier Mendivelso Sánchez, Claro Colombia, Beatriz Vetrale, Antel Uruguay; CROG Review: José Montes de PeraltaRev1, Nextel Perú, Mercedes AramendiaRev1, Telefónica Uruguay, Jack Rowley, GSMA, Beatriz Vetrale Rev1, Antel Uruguay, Héctor Huerta, América Móvil.

Common position proposal on signal inhibitors (jammers) in Latin America

Version 0.9

14 Jul 2014

*This is a **Non-binding Proposal** of the GSMA*

Security Classification: Non- Confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Executive summary

Signal blockers or inhibitors, also known as *Jammers*, are devices that generate interference or intentional disruption of communication in order to prevent exchange of information. In this case, the interference of the radio signal prevents the communication between the mobile terminal and the radio station.

Its use causes extensive disruption and alteration of cellular signal, while affecting the coverage, as well as a deteriorating service for customers. Moreover, when inhibitors production processes and installation is not strictly controlled, problems of interference may increase. In some cases, mobile users may be unaware of its terminals being blocked since the above may not be obvious until they make a call, when they would receive the warning that network is not available, thus seeing their rights to access services impaired while not receiving any communication on their mobile until they leave affected area.

Considering the serious damage generated in the network and the impairment of user rights, it is essential to control and restrict the supply of these equipments and limit their use only and exclusively in cases of public safety such as in prisons. However, we believe that in that particular case, the real solution involves controls increase and for prison authorities in each country to take appropriate measures to prevent the smuggling and use of cell phones in those precincts. On the other hand, the use of this equipment among individuals is wide spreading, causing direct damage to mobile users and companies who have purchased and paid millions of dollars for the use, development and exploitation of such a valuable and finite good as radio spectrum and network spreading.

It will also be important to establish precisely how far the responsibility of telecommunications licensees goes regarding the settlement of the damages to the signal impairment.

1.2 Scope

The GSM Latin America has followed the use of jammers with interest and concern. As in most Latin American countries, a wide range of jammers are available for purchase. Thus, inhibitors are installed in restaurants, shops, theaters, cinemas, financial institutions and others, in order to prevent customers or employees using the terminal within its facilities.

The issue of mobile signal inhibitors has been treated in different occasions by the GSMA and different aspects of its use have been covered, from regulatory issues to the security implications. An important case, we see with great concern, are the issues around the constraints of mobile services in prisons in Honduras, Guatemala and other countries in the region. However, despite its use in prisons is not new, this particular approach has not been included in the debates of the GSMA.

Mobile network operators invest heavily to provide coverage and capacity through the installation of radio base stations. Therefore, the indiscriminate use of inhibitors affect these investments since customers can not make use of mobile services in the ranges of these inhibitors.

The purpose of this paper is to provide a detailed analysis on the use of these devices in Latin America. To this end, this document has been agreed with industry, GSMA and other supranational organizations to provide a common position including the implications for the end user, which may be shared with Regulators and Telecommunications Ministries.

1.3 Definitions

Term	Description
Inhibitors/signal blockers	Radio devices that prevent mobile devices from communicating with the mobile operators radio station, therefore blocking phone calls or data transfers (SMS, internet access, etc.). These devices operate by sending out a radio signal in different frequency bands, (e.g.: 850MHz y 1900MHz) covering all mobile telecommunication technologies (2G, 3G, 4G, Satellite, etc.), as well as any other radio communication, such as television.

2 Implications of the use of inhibitors

Limitation to a specific area of use: The nature of radio signals makes it virtually impossible to ensure that inhibitors coverage is confined, for example, within the confines of a building. The are studies from the beginning of its use that show interference with base stations located up to 670 meters away from the blockers, resulting in unintended consequences such as interruption of service for legitimate users who might not be aware of what causes this. Recently, there has been evidence indicating that operators are experiencing affectations of mobile signal even more than one (1) kilometer away. This affects clients out of the intended blocked area generating service claims, and operators, by generating a bad image for degradation of service, and substantial economical losses, plus it can encourage operators to fail to comply with minimum quality standards.

Decrease of mobile coverage: Operators strive to increase and maintain the coverage and scope of their access networks as a pillar of its strategies in both directions, vertically and horizontally, especially in buildings. The use of inhibitors would go against this trend of increasing coverage and would create areas without coverage, affecting service, quality standard indicators required by governments and the rights of many users; whilst authorities of many countries mandate coverage and penalize companies that don't provide it. Sometimes it is the law in each country that mandates the network spreading and the resulting expanded coverage, to every corner of the territory, making the installation and operation of inhibitors unethical.

Insecurity increase: These devices cause a variety of interference issues that affect both the civil society, as well as law and order forces, which lowers the security provided to the public and can increase crime directly. It could be limiting the access of users to emergency services such as "911" or similar services that exist in different countries. Moreover, some applications such as alarms connected to mobile devices, or mobile personal health devices, could be interrupted by the use of inhibitors, even beyond the target coverage of these with the consequent implications of responsibility when a legitimate service is disabled without user knowledge or consent, or without public interest grounds that seek to justify it. The ubiquity with the respective terminals, prominent and important feature of mobile communications, is

threatened and diminished with the operation of the blockers, is threatened and diminished with the operation of the inhibitors.

Health and Non-ionizing radiation: Unlike mobile devices that go through rigorous certification processes according to international standards for human exposure to radio frequencies or non-ionizing radiation it has been reported that there may be problems in the use of high power for legal transmissions blocking, that may affect human health.

Several services impacted: Studies of interference made by operators show that there are flaws in some inhibiting devices that not only affect mobile phone signals but even affect other telecommunications services signal. There have been findings where some inhibitors, due to factory failure, reach to inhibit telecommunications systems in frequency bands near mobile phone operation.

Case studies on the use of inhibitors demonstrate how:

- The noise floor between bands interfered is far above the usual as shown in Figure 1:

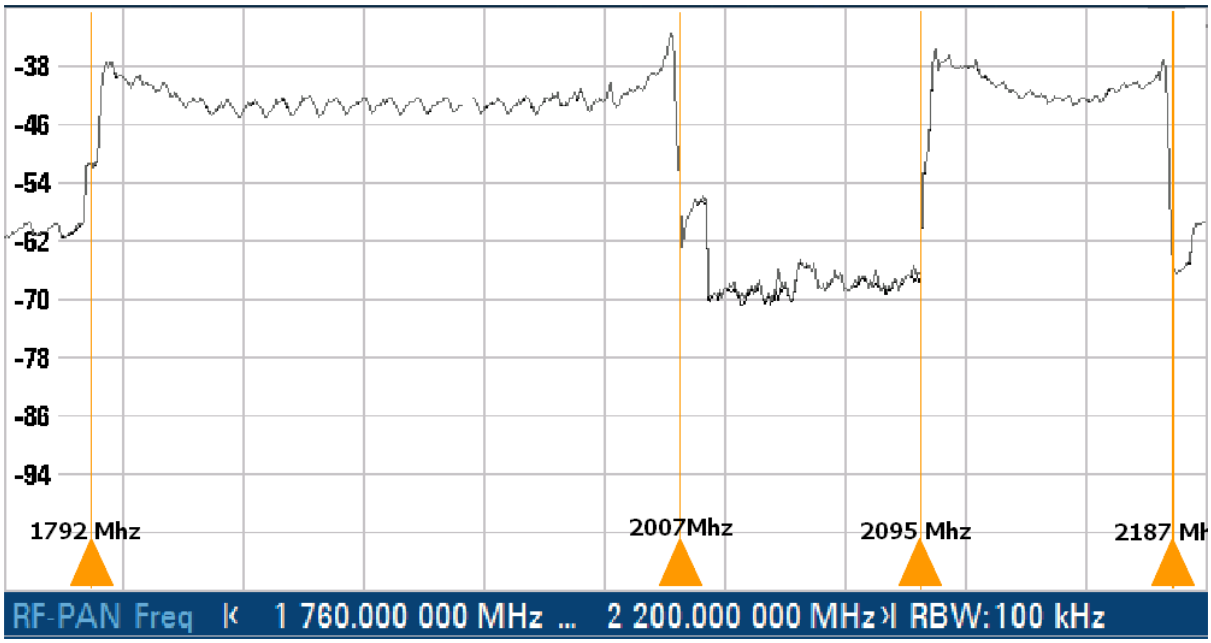

Figure 1 Increase of the noise levels due to the use of inhibitors

- Since jammers send out signals in different frequencies, they affect any mobile telecommunication technology (2G, 3G, 4G, etc.) as well as any other radio communication on the interfered frequencies. Figure 2 shows how the spectrum analyzer detects a noise level in the GSM technology, but particularly important in UMTS:

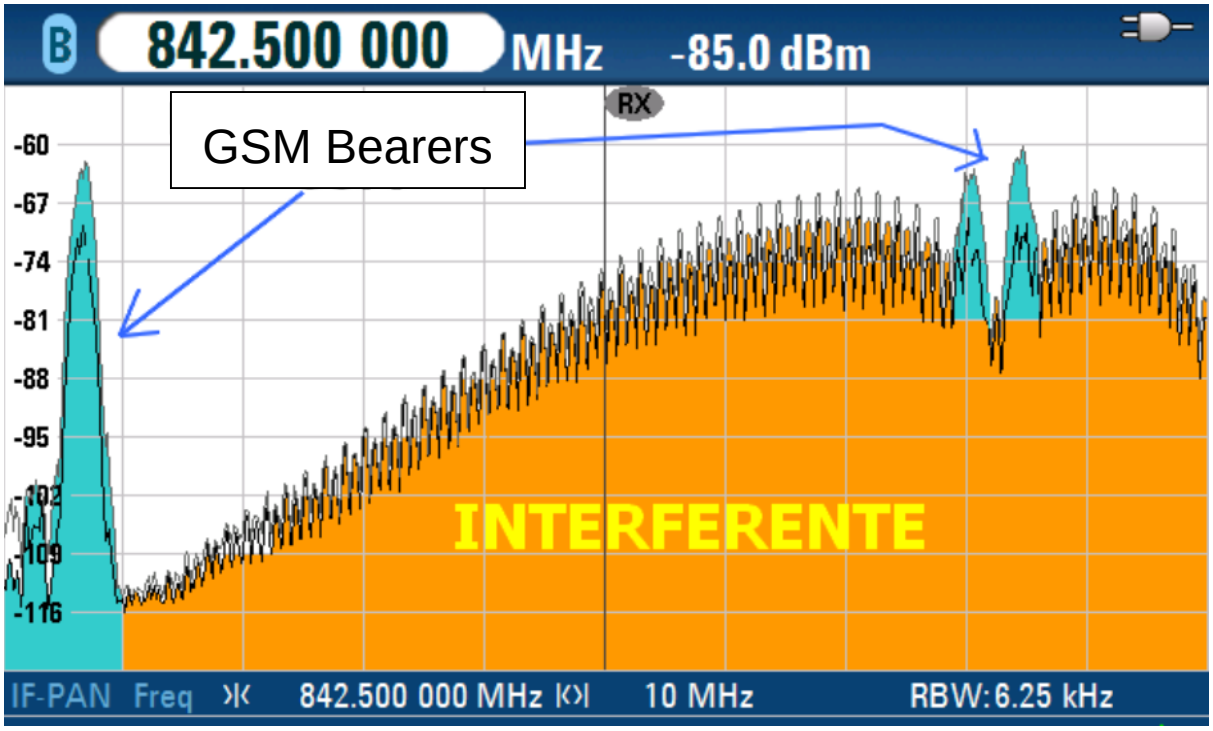

Figure 2 The interference of inhibitors affects 2G/3G

Jammers deactivation: Operators are facing cases of signal inhibitors use that are more complex and harder to detect, and even in the event of locating them, they face not only the reluctance of installing companies to deactivate the installed devices but also lack of policy that contains mechanisms or expeditious procedures for quick deactivation.

Network Quality Decrease: since jammers signal cannot be physically restricted to a specific area, a deterioration in service provision is detected around the place where they are installed, fact which goes against service initiatives promoted by regulators, the right of users to access services and operators making efficient use of spectrum, being especially critical the case where jammers are installed in buildings located within the urban perimeter in big cities.

In addition, in some markets operators are sanctioned for non-compliance with the established service indicators. It is to be noted that in some countries in the region measurements of provided service levels are being made by using applications that quantify accessibility and the number of dropped calls. In these cases, alternative solutions to signal inhibitors should be pursued or exempt the affected areas of compliance with the technical conditions required by the regulator.

The number of disconnections or drops, both voice and data, increases significantly with the presence of external noise. This level is re-established after detection and deactivation of the inhibitor; which leads to the reestablishment of a normal and stable level rate of dropped calls as shown in figure 3.

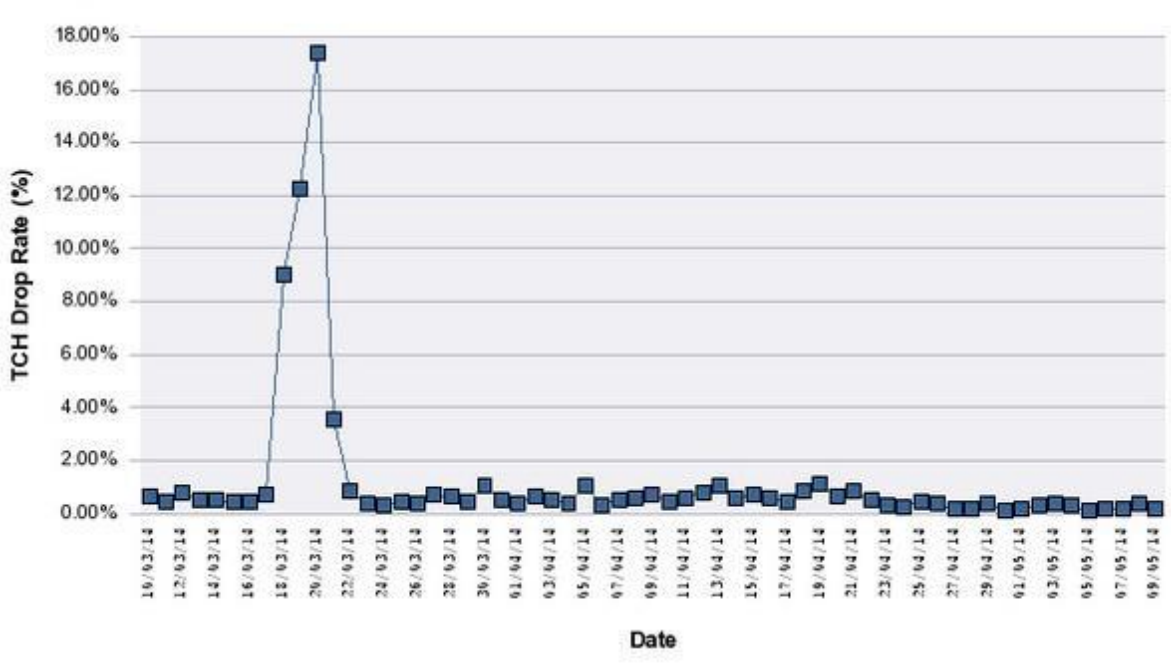

Figure 3 Increase in the number of dropped calls due to the use of inhibitors

3 Coordinated and regulated Implementation

Currently, the installation of signal inhibitors doesn't have a clear policy. The impact of its use would be substantially minimized if the coordination of its implementation with mobile operators was favoured, if its operation was controlled, and, whether their use was only allowed in cases of general interest of public safety, being specifically authorized by the Authority of each country, for which it would be appropriate to contemplate:

- Frequency transmission to be blocked.
- Technical characteristics and specifications of equipment used in the signal blocking.
- Jammers orientation for efficient blocking in the desired areas and therefore not affecting neighbouring customers entitled to have the service.
- Establishing mechanisms and/or procedures to resolve potential interference to mobile systems and users affectations.
- Location and configuration record of inhibitors, and notification to Operators.
- Requiring Homologation Certificate of inhibiting equipment to be used.
- Policy Guidelines for the use and marketing of inhibitors so that they are not arbitrarily made, requiring a specific authorization, in accordance with local regulation, limiting its range to the area that meets the legitimate security needs.
- Installation is appropriate in accordance to good engineering practices.
- Signage of inhibitors installation for the purpose of informing users.

3.1 Alternative measures to inhibitors

Given the need to restrict access to cellular networks it is deemed appropriate to evaluate other alternatives or complementary solutions either of technological or non-technological nature.

Regarding current technological solutions, there are alternative or complementary measures to the use of inhibitors to consider, as appropriate:

- Passive detection technology of active mobile devices followed by a request of restriction of use external (or integrated) to the operator's network: selective intelligent interceptors or pseudo-antennas.
- Redesign of the access network to not provide coverage in the sensitive area taking into account the peculiarities of the area to be covered, provided that it is technically appropriate, and implement "indoor" coverage with access restrictions.
- Network Monitoring: There are legal interceptions of mobile platforms that can enable the security forces to detect its activity, identify its location, and monitor traffic in those terminals to detect illegal activities, perhaps under technical schemes of geo-localization. And thus discourage handset theft by criminal gangs.
- Possible use of other nodes to intercept unwanted communications or communications originated in illegal terminals. See Annex A.2.
- Analyze traffic to locate the IMEI being used in prisons and lock through systems that allow using some IMEIs database, such as the GSMA. See Annex A.1.
- Establish a recording indicating the receptor that the call is originated in an area of "risk".
- Inspecting communications via SMS, such as detecting key words, mark spam, anti-spam filters, etc. Additionally, the GSMA offers a spam report to its members. This service enables consumers to easily report spam using a universal short code ("7726" (SPAM)) to its operator.

Among the non-technological solutions, we highlight prevention and education of the population, although the following alternatives should be noted:

- Media broadcast of modus operandi of fraudsters, as well as actions to be performed by the population in the event of being involved in one of these cases.
- The creation of phone numbers to report the numbers involved in extortion, administered and monitored by the authorities.
- Coordination between operators and authorities for the cancellation of lines involved in cases of extortion.
- Action plan for longer-term improvement in the management of prisons, with even relevant changes in the status of the different aspects in prisons (infrastructure, laws governing its operation, behaviour, codes of conduct for employees, etc.).
- Sharing information on how to detect fraud through activation patterns, distributors inclined to make massive purchases to commit fraud, recharge and recharge transfer patterns.
- Control the use of mobile services in specific locations, request for mobile to be put in silent mode, issue codes of conduct, etc. This may be the case of the financial sector and banks in which the use of inhibitors is increasing alleging security grounds, as well as libraries, where silence is pursued, or in workplaces as a way to control the use of cell phones.

Individuals and authorities have different ways of controlling the use of services, without the need to install inhibitors, for example, control the use of mobile services on site, request mobiles to be put in silent mode, issue behaviour codes, among others.

3.2 Detecting the use of signal inhibitors

Detecting the use of signal inhibitors is not an easy task. There are different methods involving the combined use of different mechanisms, including:

- Studying the databases of information on the network access of a mobile operator to analyze the noise level of a cell (Average RSSI ~ Noise measure) in the event that there has been a recent change of level in a particular area or an unusual level. In the event of an anomaly, you can proceed to a thorough study of the affected area for the location by triangulation of the noise source.

- Complaints from users who are affected by lack of access to services in certain places.

Operators may find spectrum analyzers on the market with directional antennas that provide the specific location of the frequencies inhibitor. These analyzers check the status of emissions in a wide frequency range including a large bandwidth.

In the event that the mobile network operators perform actions on the affected area and the use of these devices is verified, it is advisable for the situation to be reported to the competent authorities and governments ordered their immediate removal.

It would be important that countries explicitly regulate this prohibition, preventing the marketing and use by individuals, limiting the use specifically for cases of general interest, for reasons of public safety, in the absence of other alternatives.

4 Conclusions

The inhibition and/or interference caused by these devices affect citizens, public safety and services. Not only it does limit network coverage, but also degrades service delivery, generates harmful interference to additional services that use radio communications, increasing problems for public health officials and security, it constraints access to primary support services and can even be used to commit crimes by blocking security services. At the same time, blocking the signal does not attack the root of the problem - the wireless devices illegally ending up in the hands of inmates, who then use them for illegitimate purposes, or that the services aren't used in inappropriate areas or places. There are many and diverse alternative ways which allow compliance with this end without affecting users rights.

The GSMA and its members are committed to cooperate with governments in the region, using technology as an aid to keep cell phones out of sensitive areas, as well as efforts to detect smuggling devices, track and prevent their use.

It is vital to find a feasible solution that doesn't impact legitimate users negatively, nor affect the substantial investments made by Mobile Communications Operators pursuing coverage improvement and provision of service quality in the region.

It would be advisable that any action involving the use of inhibitors is exceptional, as a last resort, and is undertaken in coordination with operators throughout its life cycle (from

installation to deactivation) to minimize interference in the adjacencies of sensitive areas with legitimate cell phone users. Concurrently, to safeguard the public interest and proper service delivery, regulatory authorities should ban the use of inhibitors by private entities and their commercialization, and promote that both the regulation and different regional rules regarding the use of these devices take into account their effect on normal service delivery processes and quality control. In addition, the regulator in each country should assess the conformity of inhibitors, manage and keep track of the number of approved, installed and operating inhibitors in sensitive areas, and establish sanctions for individuals who use and/or market them without permission of the competent authorities.

We insist that the use of inhibitors should be exceptional, last resort, trying to make alternative arrangements that have the same goal while not affecting other users' rights.

The illegitimate use of cell phones in sensitive areas is a growing public safety problem; therefore, the mobile phone operators are committed to work with governments in Latin America to find a solution. As described earlier in this document, although the use of signal inhibitors has proliferated in recent years in various countries of the region, unfortunately this technology also interferes with legitimate wireless services/communications and other radio communication in adjacent areas.

Nevertheless, an important consideration is that attributing the responsibility to block signals to mobile operators, contrasts with their obligation to provide the service, therefore the obligation to install such inhibitors and fix the damages that they can cause should remain a requirement per se of the competent authorities.

Thus, although we share the concern of individual countries in the region on the urgent need to eliminate the illegal use of mobile services in sensitive areas, we believe that the most efficient and effective way to do that is not necessarily through the installation of devices and equipment that may affect the provision of services to third parties, or through a complex and costly regulation of monitoring, detection, suspension and lockdown of mobile lines. The States must lead the necessary actions to prevent the entry of terminals or mobile devices for the use of prison inmates.

Strengthening security to prevent illegal entry of these devices would prevent internal communication through these and therefore it is the most effective measure to eliminate the illegal use of mobile services from prisons, without affecting the rights other users who live, work or are just passing by the environment of the establishment.

Annex A Alternatives to inhibitors

A.1 Alternatives to inhibitors: stolen terminals

In some prisons crimes can be committed with stolen mobile devices. For this, the GSM technology contemplates the use of so-called nodes EIR to blacklist terminals. This allows operators to block IMEI of equipment reported stolen or lost, making significant progress in fighting fraud and theft of devices subscription. The GSMA has signed agreements with operators in different countries, as in the case of Mexico and its mobile franchisers, who must carry out everyday "black lists" with stolen DN, that followed by a report are subject to disqualification, needing the immediate signature, which confirms that was endorsed and advertised by the Presidency of the Republic and the Ministry of Communications and Transport.

Different Latin American governments have developed national databases of IMEI in order to prevent mobile devices reported stolen from being reused. Some examples are:

- Database set up by the Authority for the Regulation and Control of Telecommunications and Transport (ATT, for its acronym in Spanish) in Bolivia.
- Registry of Disabled Mobile Terminals (CEMI, for its acronym in Portuguese) in Brazil.
- Negative Data Base (NDB) by SIT (for its acronym in Spanish) of Guatemala.
- System of Activation Control and Loss of Terminals (SICAPT, for its acronym in Spanish), Conatel Honduras.
- "Agreement to prevent theft of cell phones at regional level", concluded between the 4 main operators in Mexico, Telcel, Iusacell, Nextel, and Telefónica; aimed at sharing blacklists.
- Terminals blacklist by SIGET of El Salvador and in Nicaragua by Telcor.
- Database of stolen and/or lost phones by ASEP Panama.
- Centralized database of terminal equipment stolen, lost or stolen in Peru.
- Registration and Lock mobile terminal equipment reported stolen or lost in Venezuela-2011.
- Exchange and blocking of terminals reported as stolen or lost in Uruguay.

There are also supranational solutions that allow blocking the phone outside the borders of the countries where they have been stolen. For example, GSMA offers IMEIs Database, a service provided to members, recommended by GSMA CROG, COMTELCA, CITEL and major Latin American Operators. It is a database of stolen IMEIs terminals housed centrally, which operators can log onto to upload and download data to control mobile device access to their networks.

This comprehensive IMEIs database is a key element to counteract the theft of mobile devices in Latin America and in the world. It is also a great example of how the public and private sectors can work together to address issues of specific concern to society and governments.

Despite these measures, scammers, very simply and at low cost, reverse the actions taken by operators and governments by reprogramming the IMEI. There is also the obstacle of IMEIs duplicity or multiplicity.

With regard to these practices, collaboration with manufacturers of devices for the generation of security algorithms that hinder reprogramming the IMEI is necessary. The GSMA has been working with terminal manufacturers to prevent such practices.

Detection of adulterated IMEIs and their incorporation to the IMEIs exchange between operators for blocking purposes at the EIR, is a practice that is beginning in some countries. This leads to duplication, which requires new forms of detection. It will require cooperation not only with terminal manufacturers but also with SIM manufacturers to prevent and protect legitimate communications.

A.2 Alternatives to inhibitors: Messaging

In some prisons where fraudulent courier service use is performed, it seems that even criminals often use the SMS service to extort, blackmail or conduct virtual kidnappings. There are different patterns that scammers can profit from:

- Sending spam text messages.
- Premium charge for calls or messages.
- Redirecting traffic to their URLs for other scams.
- Cheating by false gifts and prizes (computers, cars, cash).
- False claims for prepaid balance bonuses.
- Messaging received from unwanted promotions (SPAM).

Most countries have implemented measures to prevent the extortion and deception of mobile network users, victims of these crimes. As mentioned, there are different alternatives for the detection of these practices in communications by SMS such as keywords detection, trace spam, anti-spam filters, etc.

GSMA offers a spam report to its members. Reports of spam messaging of participating mobile networks are sent to this global tool that stores all the information of spam. The service also provides aggregated data from spam over mobile networks, providing better overall visibility and the rapidly evolving and emerging threats. This strategy has been successfully implemented in the region and leads not only to the detection of fraud from prison, but from other sources as SMS Spoofing or unsolicited traffic generation at locations of high value.

The spam reporting service can detect SIM cards that send spam messages repeatedly Operators can use the CDRs (Call Data Records) analysis to identify whether these SIMs follow a pattern of use in the same cell where the prison is located.

In this CDRs analysis operators can also identify IMEIs devices within the prison covered by a particular cell. These devices can be blocked using the GSMA CEIR. In these cases it is recommended the use of the spam cause code instead of lost or stolen terminals code.

Since inmates could change their SIM cards using other inmates terminals in an organized way, and these terminals could belong to different mobile operators which would change networks several times a day, it is necessary to check and block devices cross-operators.

In many cases, it may be easier to generate illegal traffic from different SIM cards than from different phones in prisons. For this reason, it is essential to maintain the visibility of the phone numbers that produce spam by spam reporting service and devices by sending spam through CEIR.

Annex B Status on the use of inhibitors

4.1 United Kingdom

Section 8 of the Wireless Telegraphy Act of 2006 prohibits the installation or use of wireless telegraphy equipment (radio) in the UK, Northern Ireland and territorial waters, Isle of Man and Channel Islands, if a valid Ofcom license is not issued or there are no regulations that exempt from the licensing requirements. It is a criminal offense by the grounds of the Crown Court that entails to a maximum punishment of two years of imprisonment and/or unlimited fines. The court may also order punishment for any device used in the commission of the offense.

The prisons rule 2012 (interference with wireless telegraphy) received Royal approval on December 19, 2012. A motion of legislative consent was agreed by the Scottish Parliament on November 8 of 2011 to extend the provision within the rules of Scotland. Provisions began in England and Wales on 21 October 2013.

4.2 Australia

In 1999 the Australia Communications Authority (ACA) issued the notification that ACA prohibited the operation or supply, or possession for the purpose of operating or supplying these specified devices known as jammers or signal inhibitors. These devices have the potential to cause significant interference to legitimate radio services including, but not limited to, mobile networks. The prohibition of these devices was established in section 190 of the 1992 rule of radiocommunications. An individual may be sentenced to imprisonment up to two years for possession, supply or operation of these devices if found guilty and organizations fined up to AU$ 165,000. Even an individual can be imprisoned up to five years if found guilty of causing interference that may endanger the safety of others or cause other person to suffer a great loss or damage, and organizations fined up to AU$ 550,000.

4.3 Unites States of America

Federal law prohibits the marketing, sale, or use of a transmitter (e.g. jammer) designed to block, overload or interfere with wireless communications. See rule of Communications 1934 and revisions 47 U.S.C. §§ 301, 302a(b), 333. Signal inhibitors can not be advertised or operated in the United States except in a very limited authorization context: official use by the federal government. For more information see http://www.fcc.gov/encyclopedia/jammer-enforcement

On May 1 of 2013 the Federal Communications Commission issued a legislative proposal (FCC 13-58) to facilitate the development of multiple software solutions based on managed access solutions to combat the use of smuggled devices in prisons. Managed access technologies use wireless based stations positioned in prison to capture and block transmissions to or from unauthorized devices.

4.4 Mexico

The current legislation in Mexico applicable to the use of these signal inhibitor devices includes the following rulings:

i. Decree amending, supplementing and repealing several provisions of the Federal Code of Criminal Procedure, the Federal Criminal Code, the Federal Telecommunications Act, the Law establishing Minimum Standards for Social Rehabilitation of Sentenced Individuals and the General Act of Public Security National System (DOF: 17.april.2012);

ii. Collaboration guidelines between Prison Authorities and Telecommunications Services licensee and Technical Basis for the Installation and Operation of Inhibition Systems (DOF: 3.september.2012);
iii. Federal Telecommunications and Broadcasting Act, Article 190, Section VIII (DOF: 14.july.2014).

The content of this regulation establishes the need to involve federal and state authorities for the cancellation of any telecommunications signal and for such blocking not to exceed 20 meters outside the premises intended (prison). Therefore, inhibitors are operated by providers contracted by the authorities, as appropriate. The legislation establishes mechanisms to solve any affectation to users, as well as evaluation and measurements mechanisms.

Is worth noting that the Merit guidelines foresee that public telecommunications networks licensees being involved in the cancellation or termination of the signals, as partners but not as directly responsible for the operation of inhibiting equipment. Also, the legislation provides that licensee perform preliminary tests, of operability and functionality, without having the obligation to block the signal, since this requirement corresponds directly to the competent authorities and providers contracted for that purpose. The guidelines contain a section on technical specifications and characteristics of the "jammers" that if fully observed palliate the difficulty of operating "inhibitors" with harmful interference well beyond the limit which the Guidelines establish.

A fundamental and crucial aspect is to establish an agreement of potential improvement and coordination between the authorities of federal and state levels for the successful implementation and effective operation of the inhibitors, to ensure the provision of the contracted service, since up to date, whilst some federal authorities have supported operators for the solution of the damages to the networks, it has not been possible to adequately coordinate and implement joint actions to correct the signal interference also at state level.

4.5 Brazil

The current rules governing the use of these signal blocking devices in Brazil are found in Resolution No. 506 of July 1, 2008, section 8.

Although this resolution regulates the use of inhibitors, additional police support would be required in order to prevent the illicit purchase of these devices and their subsequent activation by illegal businesses under the guise of increasing safety levels. Note that once installed, the identification of their use is not obvious, since the interference generated by these devices may be confused with interference from other radiating equipment or some system failure.

The content of this regulation sets out the conditions under which the equipment must operate to obtain permits for use, including the frequencies of commercial mobile services. The state government of São Paulo has carried out a tender for a system that blocks cell phone service and mobile data (Wi-Fi) in 23 of the 157 state prisons by March 2014. Brazilian government plans to spend annually to R$ 30 million (US$ 13.4 million) to install these signal blocking systems.

One aspect of potential improvement is the degradation of service in the surrounding areas where these facilities are located and therefore customer complaints. Also, existing legislation

could be modified imposing an almost total restriction on the private use of these devices, increasing penalties for noncompliance and its excepted use in specific security cases (as in prisons) being its use controlled by the administration. The rules should also define solutions that reduce the impact and interference in the immediate environment by creating standards to limit interference outside the target area.

4.6 Colombia

The current rules governing the use of these signal blocking devices in Colombia are found in the New Prison Code of the Ministry of Justice, Chapter VII. Section 110 and through Resolution 2774 of 2013 MINTIC (for its acronym in Spanish).

This regulation authorizes the MINTIC and INPEC (Ministry of Information Technology and National Penitentiary Institute) to inhibit and block mobile communications signals in prisons and jails.

One aspect of potential improvement is the entry and movement control of mobile equipment in these prisons. Besides, the implementation of these devices ends up affecting the service to surrounding areas, causing a lot of users being impacted because of these devices.

In Colombia through resolution CRC 4296 August 16, 2013, network and mobile telecommunications services providers are obliged to compensate voice service users, automatically, with monthly undertakes from 1 January 2014, for the poor voice service delivery through mobile networks due to dropped calls events.

However, it has been identified through researches the jammers and/or signal inhibitors generate impairment to the client, and operators are impacted negatively on their image and service provision. Likewise it is not easy to discriminate cases where the call is specifically affected by a signal inhibitor.

4.7 Panama

The current rules governing the use of these signal blocking devices in Panama are found in Resolution AN No. 6295-telco.

This regulation orders licensees to restrict signals (mobile telephony, PCS and Internet) at the site of prisons.

One aspect that should be improved and clarified is that the obligation of blocking is not transferred directly to operators, but for it to be a direct obligation and responsibility of authorities having jurisdiction, with the collaboration of service licensees. In addition to the above, another area of improvement in this matter is in relation to the impairment suffered by the population near prisons due to the technical complexity of restricting signals to specific areas.

4.8 Honduras

The current rules governing the use of these signal blocking devices in Honduras are found in Decree No. 255-2013, as well as the Rules of the Limitation to Cellular Mobile Services and Personal Communications (PCS) in Prisons, National Prisons and Juvenile Detention Centres at National level Law, published in the Official Gazette on May 9, 2014.

The Limitation to Cellular Mobile Services and Personal Communications (PCS) in Prisons Law prohibits mobile operators to provide services in the specific areas where penal centres or farms are located and orders antennas dismantling or to implement other technical solutions so that these places are not provided with service. Failure to comply is punishable by a fine of 20 million Lempiras (U$S 1 million) and the revocation of the concession in case of recurrence.

In addition to the above, the Rules of the Act aims to establish "technical, administrative, regulatory, and institutional cooperation and coordination mechanisms", creating a Telecommunications Security Interagency Commission (CISTEL, for its acronym in Spanish) to coordinate the implementation of technical measures integrated by: (i) the National Telecommunications Commission (CONATEL, for its acronym in Spanish); (ii) the Secretary of State for Security/ Ministry of Security; (iii) the Research and Intelligence National Bureau; (iv) Secretary of State in the Office of Human Rights, Justice, Interior and Decentralization; and (v) Operators with concession for PCS.

It is important to point out that these Rules contain some exclusive liability for operators in the performance of inhibitors, such as: (i) failure caused by vandalism, sabotage, damage or theft; (ii) failures caused by strikes, demonstrations and riots; (iii) failures caused by earthquakes, hurricanes, floods, landslides, fires or any other extreme event; (iv) failure of the power supply; and (v) occurrence of incidents and events that could be understood as ineffectiveness or vulnerability of the measures taken.

One aspect of potential improvement is that the obligation resides in the Government and not in the operator turning off cells. Also, reducing the impact caused to the surrounding population to prisons and the use of appropriate measures to restrict the entry of mobile technologies to such centres.

4.9 Guatemala

In Guatemala there is no specific regulation on the use of signal blocking devices (jammers), however two laws were issued that aim to regulate calls and the use of cellular devices from prisons, them being:

1. Decree No. 8-2013 of the Congress of the Republic *Mobile Terminal Equipment Law*
2. Decree No. 12-2014 of the Congress of the Republic – *Mobile Telecommunications Control in Deprivation of Freedom Centres and Strengthening of the Infrastructure for Data Transmission.*

About the Mobile Terminal Equipment Act (Decree 08-2013)

The Mobile Terminal Equipment Act, that came into force in October 8 of 2013, states that despite the importance of the use of mobile terminal equipment in communications in Guatemala, it can not be ignored that those goods are used as a tool to commit crimes such as robberies, extortions, kidnappings, assassinations, threats, among others, which is why within its scope it regulates the prohibition of use and possession of mobile terminal devices and any type of technology that uses SIM card, Micro SIM or any other type of mobile communication in all detention centres, prisons and correctional facilities, for both minors and adults.

The mentioned law, empowers the Ministry of Interior to request from mobile operators reports of phone numbers that, according to their research, might be generating traffic from places of deprivation of liberty of any kind, imposing on the operator the obligation to inform, in accordance with their records, the telephonic traffic of the requested numbers that could be being generated from a cell that is next to a detention centre of any kind.

This legislation creates certain offenses related to the use and entry of mobile terminal equipment to detention centres, which are:

- Use of mobile terminal equipment in places of deprivation of liberty. (Art. 26)

  Whoever is being held in any detention centre and illegally possesses or uses a mobile terminal and/or any electronic equipment that used for communication shall be punished with imprisonment for 6-10 years.

- Entry of mobile terminal equipment to detention centres. (Article 27).

  Whoever enters mobile terminal devices and/or components or any electronic equipment used for communication to detention facilities, shall be punished with imprisonment for 6-10 years.

- Use of mobile terminal equipment by government officials and employees. (Article 28)

  Public officials or employees of places of deprivation of liberty who carry, use, facilitate or enable the entry of mobile terminal equipment or any electronic equipment that is used for communication to places of deprivation of liberty shall be punished with imprisonment of 6-12 years and disqualification for crimes against public administration.

From the above it is clear that such regulatory body is an attempt to regulate and prohibit communications originated from places of deprivation of liberty, but as mentioned ut supra it is not a direct signal inhibitors regulation.

Mobile Telecommunications Control in Centres of Depravation of Freedom and Strengthening of the Infrastructure for Data Transmission Law. (Decree 12-2014)

This Law, which came into force recently (April 25, 2014), states as a matter of general and national interest the control of mobile telecommunications in prisons, including specialized facilities for serving custodial sentences for juveniles in conflict with criminal law.

Article 3 regulates telecommunications control in prisons where operators are ordered to implement technical solutions (inhibitors are not explicitly mentioned) so that traffic of mobile telecommunications cannot be generated from prisons. This obligation is mandatory for all operators providing telecommunications services in Guatemala.

Prison authorities undertake periodic monitoring every two weeks, to ensure that the measures implemented by the operators are effective. In the event of noncompliance, the regulator will impose on operators fines approximately from US$ 38,000 to US$ 65,000 for each centre and month in which the measure imposed by the rule is not satisfied.

Is worth noting that the law expressly exempts operators by stating "they will have no liability of any kind against users of telecommunications services that are affected by the implementation of these measures" and sets implementation to be done within 8 months of the law coming into force.

The Ministry of Interior and the Ministry of Social Welfare of the Presidency are obliged to provide all the support required to implement technical solutions.

It is clear from this legislation that it is the operator's obligation to implement technical solutions to avoid mobile communications from prisons.

It is important to work on the fact that the obligation of public safety must reside in the Government of Guatemala whom through the authorities of the Ministry of Interior and Penitentiary System, entities with expertise in security and detention centres, should be responsible of implementing these solutions and to prevent any crime that is generated from the detention centres, counting of course with the support of operators in communications.

Note that prior to this legislation, the Government implemented jammers in some prisons, which were not efficient since it was easy to handle for prisoners, and they affected not only the area surrounding the prisons but also significant distances from where they were installed.

The implementation of such measures is subject to the issuance of a resolution by the Superintendence of Telecommunications, with prior notice to the Telecommunication Business Council.

4.10 El Salvador

The Telecommunications Law Reform Draft is currently in process of consultation, and the government's proposal relates to the topic of strengthening the security based on the absence of signal in prisons. The draft reads:

"Obligation to restrict telecommunications signals in prisons" in Article 42-J says: "Operators of telecommunications networks will be required to adjust the intensity of their signals at a lower or equal level at minus eighty-five decibels relative a mili watt (-85 dBm), with tolerance of plus three decibels (db +3) within the penitentiaries and rehabilitation centres for minors and should prevent its radiant systems being oriented to or run their direct signals or exclusively to the interior and perimeter of the centres". Failure to comply with this provision shall result in appropriate administrative or legal consequences.

This legislation largely affects the quality of service of users near prisons because they are located in populated urban areas. Due to the technical complexity of signal restriction to specific areas, national operators have proposed a different solution to prevent mobile service within prisons such as the use of silent sectors in close proximity of the prison.

In addition, it is requested for the government to implement measures of total control on the entry of phones, chargers, cables, batteries, and others, to restrict any call attempts. An important point is the "filter" of staff and guards that respond to the interests of the Prison, not the inmates, especially in discretionary management of Inhibitors.

4.11 Peru

The rules governing the use of these signal blocking devices that are in force in Peru are found in the Supreme Decree of the Ministry of Economy and Finance number 012-2012-MTC.

This regulation mandates the installation of signal jammers in thirty-three prisons in the Andean country. The measure is accompanied by the installation of additional technologies such as camcorders, scanners or biometric records. Additionally, the implementation of extra security systems that enable identifying the penal centre from where the attempt to make the call is made is expected.

Pursuant to what is stated in this rule, the Peruvian State in early July 2014 has licensed the installation and operation of cell phone and Wi-Fi signal blockers in 33 prisons nationwide, each one having over 400 inmates.

This bid, which is expected to be completed in late June 2014 and was originated by presentation of a private initiative, is one of self-sustainable nature, since the investment is recovered by prisons public telephony service fee charges.

On the other hand, it is important to note that in Peru there is also a regulation issued by the regulatory body (OSIPTEL, for its acronym in Spanish) that seeks to detect, block devices and suspend those mobile lines that engage in prohibited use within prisons, this matter can be revised in Executive Committee Resolution Nº 112-2011-CD-OSIPTEL. According to this rule, analysis of the cases of prohibited use relies on operating companies. To do this, they must carry on daily actions and in a continuous way in order to detect whether mobile lines that meet the following performance parameters actions are present in their network: (i) as a mandatory criteria, the lack of mobility of the mobile terminal for 7 days, being covered only by stations that at the same time cover prisons; and (ii) as optional criteria, outbound high dispersion (90%) or recurring SIM Card change and/or atypical communication schedule. Whenever operating companies detect and suspend service for prohibited use they must notify OSIPTEL and the Ministry of Interior. They should communicate the reconnection of a previously suspended service if the subscriber appeared before the operator showing the SIM Card and equipment used, or if provided documentation demonstrating that lives or works near a prison.

4.12 Uruguay

On October 9, 2000, the National Communications Authority issued a resolution by which it was established not to approve or authorize the installation or operation of equipment acting as "mobile phone neutralizers" and/or any similar devices in the country, which purpose is to cause harmful interference in a wide range of frequencies.

However, for over a year strong and multiple interferences have been identified, generated by blockers installed by individuals, companies, mainly financial, to prevent the use of phones by their employees and/or customers on their premises.

It is if our understanding that equipment has been purchased online, at shops or directly brought from abroad by users.

The installation is done directly by individuals or by some technician. The interference generated by these devices always affects people outside the intended area, and in several

cases it has been identified that they were configured incorrectly, generating extremely harmful interference to the entire network, and blocking radio communication up to 200 meters.

Several months ago the Telecommunications Chamber of Uruguay reported this issue to the Regulator, allowing disabling some cases working together with both the Regulator and companies.

It is essential to control and restrict the supply of these equipmentsincreasing the controls, disabling the option for individuals to use these devices, while they cause a direct harm to other users and services, while limiting access and affecting safety of all.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.9	June 16th 2014	New paper on signal inhibitors	CROG	José Antonio Aranda, GSMA

C.2 Other Information

Type	Description
Document Owner	CROG Latam
Editor / Company	José Antonio Aranda, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org

Your comments or suggestions & questions are always welcome.