Roberson and Associates, LLC
Technology and Management Consultants ®

CONTRABAND PHONE SOLUTION ASSESSMENTS:

COMPARISON OF THE USE OF MANAGED ACCESS V. PRECISION JAMMING SYSTEMS IN CORRECTIONAL FACILITIES

B. ALBERTH, M. BIRCHLER, N. NATARAJAN, B. PAYNE AND D. ROBERSON

2 FEBRUARY 2018

V5.0

Table of Contents:

1 EXECUTIVE SUMMARY

This paper examines the use of Managed Access Systems (MAS) and precision jamming systems as alternative methods of effectuating denial of service to contraband devices within correctional institutions. A description of example correctional facilities is provided, which includes the highly complex radio frequency (R.F.) environments, multiple cellular spectrum bands, and several technologies that must be addressed. The Managed Access and precision jamming systems are then described with particular focus given to their R.F. coverage footprint requirements, methods of service denial, and impact on local commercial wireless networks. Core networking connectivity and forensic features are also described.

The concept of precision jamming is introduced as it is required that jamming must not cause any degradation in service to commercial wireless networks outside of the prison boundary. Jammer denial of cellular service inside the prison boundary may also become unacceptable due to the increasing reliance of public safety and first responder service on commercial wireless networks (i.e., FirstNet). That is, with the introduction of FirstNet, First Responder communications services will be carried over commercial wireless networks. Thus, it is imperative that R.F. jamming systems not degrade these critical communications.

It should also be noted that, regardless of the ability to contain jamming within the prison boundary, jamming is an "all or nothing" approach. It is not possible to limit jamming to contraband devices while allowing use of legitimate devices. Instead all devices would be jammed, including those attempting to reach 911 services in an emergency.

It is found that for each system there are common R.F. engineering methods and techniques used to address these focus areas. It is also found that there is very little functional differentiation between network elements employed within the two systems, except for the core network which is applicable to MAS systems only. Small, medium, and large sized facilities are defined and relative costs are analyzed for all three cases.

The summary of our results is that in a large facility, precision jamming is expected to be costlier than a MAS due to higher system management and monitoring costs, as well as higher R.F. jamming head-end costs. In a medium facility, the precision jamming system's higher management and head-end costs are expected to be partially offset by the MAS core network costs. In a small facility, the additional cost of the MAS core network may make it slightly more costly.

Overall there is very little difference in capital and operational costs between Managed Access and precision jamming systems. Operationally however there is an enormous difference in that a jamming system is effectively a very "blunt instrument" approach to the problem while the MAS approach is more of a "versatile tool" that has numerous other diagnostic benefits enabling prison officials to gain a valuable perspective on the wireless activity in the prison and to use this information as appropriate to detect and deter not only wireless misuse, but potentially other contraband and general criminal activities.

2 INTRODUCTION

2.1 Background

Unauthorized use of contraband wireless devices in correctional facilities has led a variety of stakeholders to call for the investigation and implementation of a number of possible solutions, two of which are Managed Access Systems (MAS) and precision jamming. For several years, MAS solutions that deny service to contraband devices have been successfully deployed in correctional facilities. On the other hand, precise jamming systems that deny service to contraband devices have not been deployed in the U.S. for a variety of reasons [1].

One question that arises in this proceeding is the relative complexity and costs of jamming-based systems as compared to MAS. This paper examines this question. Per the subsequent sections, it is found that the complexity of precision jamming is comparable to that of Managed Access. Furthermore, precision jamming may prove even more technically challenging than a MAS because of the potential harmful impact on other wireless communications networks.

2.2 The Correctional Facility Environment

Correctional facilities, both publicly and privately managed, vary widely with regard to size, architectural design, security level and location to name just a few factors. Due to these and other sources of variation, R.F. systems targeted on these facilities will require custom design, installation, maintenance and management. The following figure provides information for two relevant facilities, those being the Federal Correctional Institution, Cumberland Maryland and the Dallas County Detention Center, Dallas, Texas.

Figure 1. Federal Correctional Institution (Left) and Dallas County Detention Center (Right)

Note that whereas the Maryland facility is surrounded by a primarily rural environment, the Texas facility is embedded within an urban environment.

Figure 2 shows selected locations within the Maryland facility.

Figure 2. Federal Correctional Institution, Cumberland Maryland: Interior Views

These figures illustrate numerous correctional institutional features, including:

- Building(s) within a well-defined security perimeter (Figure 1)
- Highly variable environments directly outside of the security perimeter (Figure 1)
- Staff areas (Figure 2, Left)
- Multiple small cells with metal doors and thick walls (Figure 2, Center)

  Note that there will be significant variation in cell construction and layout as a function of prisoner security level.
- Common areas used by prisoners and staff (Figure 2, Right).

These features create context for the following solution assessments.

2.3 The Radio Frequency (R.F.) Environment

Any contraband phone service denial system must operate in a highly complex R.F. environment. The following two sections discuss two primary areas that give rise to this complexity and are applicable to both solutions under consideration.

2.3.1 Spectrum and Technologies

Cellular systems operate in multiple spectrum bands using numerous generations of technology. Cellular spectrum bands include allocations at: 600, 700, 850, 1700, 1900, 2100, 2300 and 2500 MHz. Cellular technologies in use today are 2G (GSM, CDMA), 3G (UMTS) and 4G (LTE). Each of these technologies uses a specific channel structure. For example, GSM uses 200 kHz Frequency Division Duplexing (FDD, separate uplink and downlink channels), while LTE uses multiple channel bandwidths (i.e., 1.4, 3, 5, 10, 15 and 20 MHz) and both FDD and Time Division Duplexing (TDD), which utilizes a common uplink and downlink channel.

Cellular phones also generally include non-cellular technologies such as Wi-Fi and Bluetooth. In addition, satellite phones (e.g., Iridium and Globalstar) may provide wireless access to services from certain areas within the walls of a prison complex. These technologies can be used to access wireless services without need for communication with cellular base stations.

Currently, fifth generation (5G) cellular technology is in the early stages of definition and standardization. 5G technologies will utilize additional spectrum bands with their own specific propagation characteristics and channel structures. Thus, the current spectrum framework is already complex and will become more so with the deployment of next generation systems.

A prison precision jamming system must prevent all of the above cellular and non-cellular communications with no impact to other mission critical systems such as public safety. Therefore, high performance filtering will be necessary to achieve this requirement.

This spectrum complexity and evolution creates significant challenges when designing and managing a precision jamming system. That is, the precision delivery of jamming signals to new spectrum bands/channels and for new systems may require costly upgrades to jamming devices and systems. For example, a recent article on jamming systems in India noted that existing prison jamming systems didn't work on newer wireless technologies that are used for 3G and 4G communications [2].

Of course, MAS systems will also require upgrades as new cellular technologies roll-out. However, a MAS solution is designed to enable efficient evolution since they are constructed using cellular technology platforms and therefore, may not require as extensive upgrades as precision jamming systems would.

2.3.2 R.F. Propagation Issues

Although R.F. propagation has been measured, studied and modeled for generations, actual behavior in specific cases remains difficult to accurately predict. Areas of uncertainty include equipment (e.g., antenna patterns, non-linarites, and filtering), propagation modes (e.g., diffraction, reflection, absorption, and scattering) and environment (e.g., building walls, windows, foliage, and terrain). Therefore, although a powerful body of modeling science is at the disposal of R.F. system designers, the need remains for substantial testing and validation. Propagation also varies with frequency. As new spectrum bands are deployed with commercial cellular service the propagation in the new band needs to be measured and modeled.

Outside of laboratory conditions, it is virtually impossible to constrain the extent of R.F. signal propagation to well-defined geographic areas. Generally, the power of propagating R.F. signals falls off with distance from the transmitter. The rate of this power reduction with distance depends on many factors as referenced above. As a consequence, when designing R.F denial of service systems such as precision jamming, there is the high likelihood that the R.F. signals will also propagate into undesired areas.

The difficulties associated with controlling R.F. propagation beyond an outdoor perimeter are well understood by the wireless engineering community. Precision coverage control requires sophisticated design and modeling capabilities, directional antennas, complex deployments and active, continuous validation, testing and management. This issue is of particular sensitivity for jamming systems, as any R.F. energy leakage beyond the correctional facility perimeter can significantly degrade or outright block legitimate wireless communication by the general public.

3 SOLUTION ASSESSMENTS

This paper is not intended to provide a comprehensive overview of all potential contraband phone service denial solutions. Rather, it provides focused assessments for two solutions of current interest, those being Managed Access and precision jamming systems. As has been discussed above, precision jamming systems have not been deployed in the U.S. and hence, the following discussion of jamming systems is generally theoretical in nature.

3.1 Managed Access Systems

MAS systems use commercial wireless spectrum to capture and prevent contraband phones from being used inside a prison facility and require wireless carrier consent, including spectrum leases, prior to deployment. In other words, managed access technology is used to establish a Radio Access Network (RAN) that serves as a multi-carrier, multi-band cellular network within the prison facility.

3.1.1 General Considerations

A MAS appears to its users as a standard operating commercial wireless network. Figure 3 shows a conceptual overview of a MAS. The region inside the red ellipse represents the area of a prison facility from which legitimate and undesired calls may be attempted to one or more commercial networks. The figure shows an example with two commercial networks, labeled Network 1 and Network 2. Note that inside the prison boundary two of the three cell phones are authorized to communicate while the third is unauthorized. Therefore, the unauthorized phone must be blocked. Finally, the cell phone outside the prison boundary must be able to communicate without impairment by the nearby MAS system.

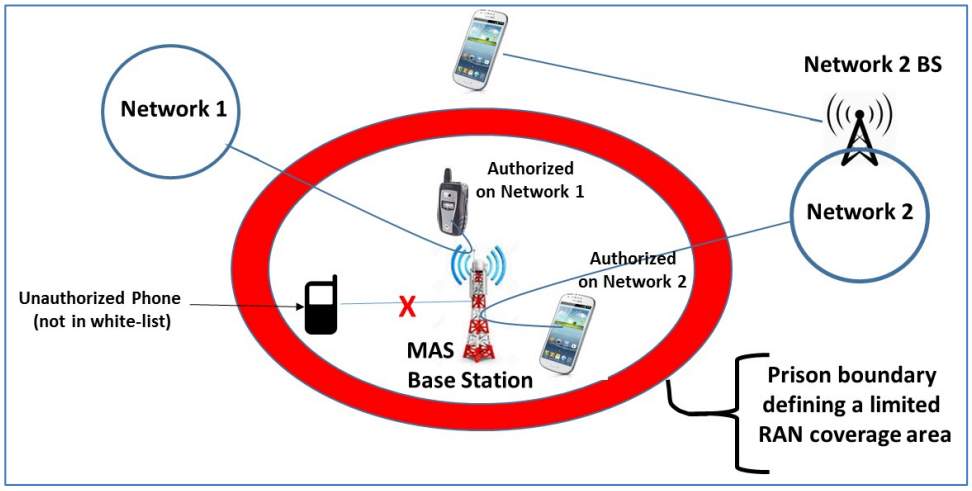

Figure 3. Conceptual Managed Access System

3.1.1.1 Coverage Footprint Requirements

A key MAS requirement is that the coverage footprint must be very near to 100% for the solution to be effective. Thus, if the system design is only 99% effective, there could be significant areas in which prisoners could still make illegal calls. A MAS must coexist with the commercial networks in the areas immediately surrounding the prison facility. Successful MAS deployments require accurate control of the footprint of the radio access coverage through a variety of techniques (e.g., architecture design, power control, distributed antennas, directional antennas, sophisticated repeaters, and other radio parameters and technologies) such that the commercial coverage is not impacted outside of the prison facility. An effective MAS is adaptable to the prison facility, whether it be urban or rural, and the local commercial radio environment.

3.1.1.2 Denial of Service to Unauthorized Devices

A Managed Access network is designed to present the "dominant" network signal within its limited authorized RAN coverage area (see Figure 3). The MAS signal is intended to overwhelm signals from nearby commercial network base sites within the boundaries of the correctional institute. A

MAS appears as an extension of local carriers' networks and intercepts (or captures) cell phone signals as calls are attempted from within a prison facility.

Once captured, unique identifying information is compared against a list of known authorized devices. Only transmissions from devices that are in the authorized list will be redirected to the commercial system and allowed to connect, while the call attempts from phones not on the authorized list are held by the MAS system, effectively preventing them from reaching commercial cellular networks to complete their attempted calls.

SMS and data calls are managed the same way, devices on the authorized list are permitted to send/receive SMS messages and data. Unknown phones (i.e., those not on the authorized list) are prevented from accessing the commercial networks and thus cannot surf the web, make/receive calls or send/receive SMS.

A MAS can also permit completion of 911 calls even if the cell phone is not on the authorized list. Thus, a MAS provides the appropriate balance between the control of contraband devices and permitting approved users to continue the use their device in the same restricted coverage area of a prison facility while still allowing emergency calls to complete properly.

For a MAS system design, as long as any R.F. signal leakage beyond the correctional facility perimeter is lower in power than that provided by the external cellular network, there will be minimal chance of service degradation to the general public. This condition can be ensured through proper design and deployment of the MAS system.

3.1.1.3 Interaction with Local Commercial Wireless Networks

Whereas a jamming system seeks to prevent service to all users in a prison facility, a MAS works by selectively blocking a group of users from using wireless networks to communicate. A well-designed MAS system can eliminate the potential for interference to users outside a prison facility or in adjacent bands. The cost of a MAS is a function of the size and complexity of a prison site as well as its location (e.g., urban, suburban and rural).

3.1.2 Practical Experience

In a specific urban deployment, wireless service denial was required in a tightly defined area, so coverage was implemented with a Distributed Antenna System (DAS) [3]. The following list contains core design tasks necessary for practical implementation of a DAS-based MAS:

1. Fine-tuning the radio signal footprint - prison facilities are constructed using materials that block and reflect signals in very unpredictable ways resulting in potential MAS network coverage "holes".
2. Refining the authorized device list – create and update the list to keep it up-to-date.
3. Hardening MAS hardware and associated infrastructure against environmental factors as well as to secure against destructive actions by inmates.
4. Addressing location-specific unique characteristics including facility-specific physical constraints and characteristics of the local commercial wireless network environment.
5. Ensure that the contraband phone cannot gain access to and service from the local commercial wireless network.

3.2 Precision Jamming Systems

Interest in the use of "jammers" has been expressed by some correctional organizations due to the assumption of lower cost and complexity (see [4], [5], [6]). However, these assumptions must be assessed with respect to the necessary system requirements, wireless engineering realities and legal/regulatory barriers. A "jamming device" (as opposed to a "jamming system," which is the topic of this paper) transmits on the R.F. channels used by cellular base stations to disable the communication link with their associated cell phones. Note that a "jamming system" uses "jamming devices" as a key component in an overall system solution.

Our scope excludes readily available, inexpensive, commercial off the shelf (COTS) jammers such as the example shown in Figure 4.

Figure 4. Example COTS Jammer

This is because use of COTS jammers will create uncontrolled outputs, leading to unintended consequences such as significant disruption to other wireless systems. The use of cheap, COTS jammers distributed throughout a facility cannot provide complete coverage without causing debilitating interference to wireless systems inside and outside of the facility's security perimeter. That is, the uncontrolled R.F. emission of these devices and lack of proper system design will allow R.F. energy to "leak out" into the surrounding environment, negatively impacting many other wireless systems, including mission critical wireless systems inside and commercial systems outside the facility. As a specific example, Monstrol 10, featured in Figure 4, jams not only cellular channels, but also GPS, Wi-Fi, Bluetooth, Lojack, etc. A COTS jammer could also disrupt mission critical wireless communication within the prison.

Likewise, small jammers intended to provide very localized disruption will not be effective at blocking use of contraband devices. As discussed above, the complex structural and RF prison environment would mean that localized jammers could be easily avoided by a prisoner moving away from the device – likely only a few feet or around a corner. Accordingly, such localized jammers are not considered because they do not address the underlying concern.

Therefore, we here compare solutions that satisfy the requirements of all stakeholders interested in combating illicit cell phone usage without harming the legitimate interests of any stakeholder community (both the corrections industry and the mobile carrier industry). The "precision

jamming" system is designed to meet these requirements, thus making it the jamming alternative upon which this paper will focus.

3.2.1 General Considerations

To provide effective denial of contraband phone use, a complete wireless system of jammers must be designed, deployed, managed and maintained. Thus, an effective precision jamming system will have significant commonality with MAS.

3.2.1.1 Coverage Footprint Requirements

A key jamming system requirement is that the coverage footprint must be very near to 100% for the solution to be effective. Thus, if the system design is only 99% effective, there may well be significant areas in which prisoners could still make illegal calls. It is in prisoners' interests to find these areas, so it should be assumed uncovered areas will be sought out and used by inmates when possible. For example, in a correctional facility of size 1,000 by 1,000 feet (or 1 million square feet), a 99% effective goal would leave 10,000 square feet of space in which calls could still be made. Thus, if the goal is to ensure that contraband phones cannot be used within a correctional facility, a precision jamming coverage goal would likely be closer to 99.99%. A sophisticated management system will be required to ensure that all jammer devices are operational and performing to specifications in order to maintain this level of coverage.

3.2.1.2 Denial of Service to All Devices

By their very nature jamming systems deny wireless communication to all users. Therefore, legitimate personal and professional wireless communication will be prevented along with use by prisoners. Given the scope and depth of wireless communication's support of applications for work, safety and awareness, denial of these services to legitimate users can create issues of organizational effectiveness and safety. Regarding the latter, jamming systems will also block 911 calls which are essential for effective response to emergency situations and may violate 911 regulations.

For example, the FCC, in its 4th Report and Order setting wireless E911 requirements [7], has noted its tangible benefits of improving location accuracy with respect to personal safety and protection of property. Jamming systems will nullify any such benefits.

3.2.1.3 Degradation of Local Commercial Wireless Networks

Due to the nature of R.F. propagation, it is virtually impossible to design a jamming system that effectively blocks all wireless communication within the correctional facility boundary while causing no degradation to wireless systems operating outside of the boundary. Due to well accepted commercial wireless engineering design considerations, wireless networks are designed with carefully controlled "margins" for connection reliability. In other words, the equipment and supporting systems necessary to enable reliable communication links to a targeted coverage area are designed to provide service at low signal strength, thereby extending a particular cell tower's coverage area. Thus, while the deployed commercial wireless system is designed to ensure reliable links between the base station and phone, there is not an excessive "margin for error", especially at cell's coverage edge.

Therefore, when R.F. jamming energy propagates beyond the correctional facility's security perimeter, it can cause significant degradation to outside commercial wireless system performance. Thus a "perfect" jamming system would create high power R.F. interference within the correction facility's perimeter and near zero R.F. power outside the perimeter, a design that would be virtually impossible to implement. R.F. energy from the jamming system will certainly propagate beyond

the perimeter and, in many cases, create sufficient interference in the surrounding commercial system to significantly degrade performance or even prevent reliable connections from being established. In other words, the unplanned interference caused by the precision jamming system will overwhelm the "margin for error" built into the commercial system. This degradation can occur even for facilities in rural areas, particularly if there are nearby areas where one can expect legitimate commercial wireless activity, for example, highways.

As a consequence of these effects, precision jamming R.F. system design must minimize any negative impact on nearby commercial systems. This design will require coordination with all potentially affected commercial operators with regard to interference levels and Key Performance Indicators (KPIs). A reliable, low delay management process will also need to be established and maintained over the jamming system's lifetime to ensure that interference issues are quickly identified and resolved. Thus, a sophisticated management system will be required for a practical precision jamming system.

Finally, the precision jamming system must be designed to have no measurable negative impact on spectrum bands used by the correctional staff for communication. In particular, public safety wireless communication systems must be completely unaffected by the jamming system. Further, with the introduction of FirstNet, First Responder communications services will be carried over commercial wireless networks. Thus, it is imperative that R.F. jamming systems not degrade these networks.

3.2.2 Practical Experience

Although use of jammers is generally prohibited in the United States, there is available information regarding their practical use in correctional facilities.

3.2.2.1 NTIA Testing

On May 12, 2010, the Department of Commerce published a Notice of Inquiry in the Federal Register titled "Preventing Contraband Cell Phone Use in Prisons." The following extracted text (emphasis added) relates to the issue of jammers [8].

> Telecommunications and Information Administration (NTIA) seeks comment on technical approaches to preventing contraband cell phone use in prisons. Congress tasked NTIA with developing, in coordination with the Federal Communications Commission (FCC), the Federal Bureau of Prisons (BOP), and the National Institute of Justice (NIJ), a plan to investigate and evaluate how wireless jamming, detection and other technologies might be utilized for law enforcement and corrections applications in Federal and State prison facilities. To assist in its evaluation of these technologies, NTIA requests information from the public on technologies that would **significantly reduce or eliminate contraband cell phone use without negatively affecting commercial wireless and public safety services (including 911 calls and other government radio services)** in areas surrounding prisons.

The NTIA conducted extensive testing of jammers resulting in numerous issued reports [9], [10], [11], [12]. Although summarizing this extensive effort is beyond scope for this paper, we have drawn the following two points from this body of work:

1. Although use of jammers is substantially prohibited in the United States, this NTIA work has created a resource from which R.F. issues associated with jamming systems can be identified and assessed.
2. Even for these extremely limited tests, practical information on jammer impact to nearby commercial wireless systems was generated.

The focus here will be on point 2. The following excerpt from [9] indicates that even for the extremely limited jammer device tests at the Cumberland facility (see Figure 1 (left) and Figure 2), nearby commercial wireless operators reported measurable and significant degradation to their network performance.

> The wireless carriers express concern about the interference that jammers could cause to in-band cell phones, based upon the NTIA tests at the Cumberland, Maryland facility. In its comments, Sprint Nextel contends that after analyzing data gathered at one of its cell sites, interference may have occurred to cell phones attempting to communicate with that cell site. Sprint Nextel notes that this cell site provides coverage to the area immediately north of the jamming zone. Additionally, Sprint Nextel states that during the test period, there was a "definite trend upward in the rate of dropped calls and a trend downward in successful call attempts." Verizon Wireless concludes that "signal measurements from the NTIA jamming tests taken at the furthest distance outside the prison from the jammer location are strong enough to cause harmful interference to commercial mobile subscriber devices." Other carriers note their concerns over the results of the NTIA testing and the potential for interference.

Note that these negative consequences resulted from testing of a jammer device as opposed to a jamming system which consists of numerous devices deployed throughout the entire prison. Therefore, we expect that a deployment of a poorly designed system consisting of numerous jammer devices would pose a far greater threat to external wireless systems than did this limited test.

3.2.2.2 Other Countries

Jammers are legal in other areas of the world where they have been used in many venues, including prisons. Based on these deployments, the GSMA published a paper titled "Common position proposal on signal inhibitors (jammers) in Latin America". Based on this practical experience the GSMA stated the following:

> 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.[13]

The authors, based on this practical experience, go on to make similar arguments against use of jammers as have been included in this paper. For example, the following figure has been extracted which shows the significant negative impact on call-drop rate due to being in-range of a jammer device.

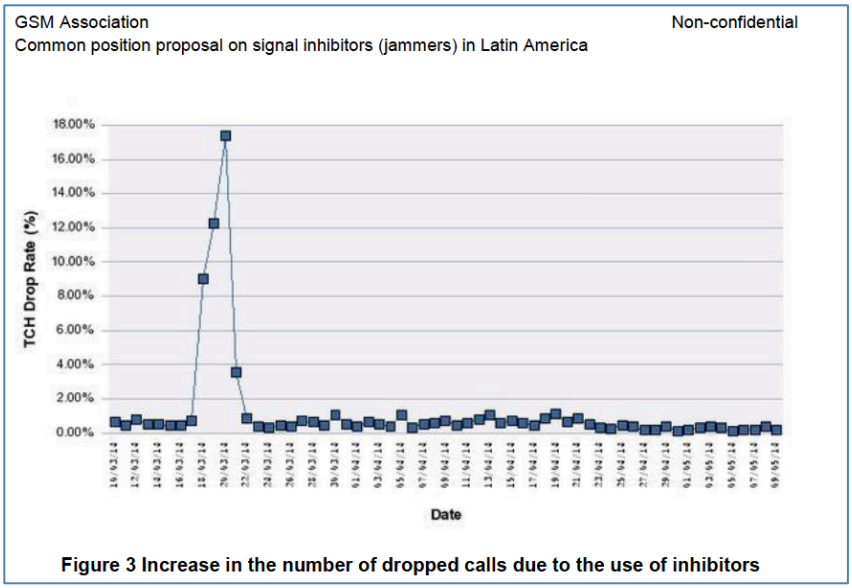

Figure 5. Extracted Figure from [13]

This figure shows a time plot for "dropped calls" by a cellular system in the vicinity of a "jammer." A "dropped call" denotes a defect in which the cellular system is unable to maintain the wireless link during the call, and thus the call is prematurely terminated (i.e., before the entities in the call have finished their communication). While the "jammer" is turned off this severe quality defect occurs at well below 2% of the time. However, when the "jammer" is turned on this defect skyrockets to almost 18%. In other words, with the "jammer" on almost one in five calls will prematurely terminate. Thus, the issues that have led to banning jammers by non-federal entities in the United States have been confirmed by the practical consequences of these disruptive devices in Latin America.

The GSMA paper addresses numerous technical and policy issues related to use of jammers. The following paragraph from the Conclusions section summarizes their findings, which are based on practical experience.

> The inhibition and/or interference caused by these devices affect citizens, public safety and services. Not only it does [*sic*] 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. [13]

Additionally, in a recent *The Sun* article on prevention of contraband cell phone use in UK prisons, "fears that traditional jammers could take out the mobile phone signal in entire neighborhoods close to a prison" were discussed [14]. Due to these legitimate concerns, a trial system with sophisticated technology that can "create a huge virtual filter that detects any handset that hasn't been approved by a prison governor and then blocks the signal" is being tested.

4 COST COMPARISON

In this section, we provide a relative cost comparison between Managed Assess and precision jamming systems. Generation of a comparison with specific dollar costs would require identification of a specific correctional facility for which the systems are targeted, performance requirement definition, design and modeling work, component and system costing and OPEX estimation.

4.1 Correctional Facility Sizes and Characteristics

Correctional facilities come in many sizes and are located in diverse areas, from rural to dense urban. They also have a wide variety of purposes and house a wide array of inmates with unique needs for support and supervision. These needs often have significant impacts on the physical architecture of the facility, the inmate to staff ratio, the risks associated with the inmate population, and the relative freedoms that the inmates enjoy. For example, medical service areas present particular challenges due to the use of electronic equipment that supports health and life. Finally, the facility's age can cause significant design variation due to changes in building materials, layout and A.C. power availability.

This complexity does have a significant impact on the challenge associated with designing an appropriate system to mitigate the contraband phone challenge. A detailed discussion on this set of topics is beyond the scope of this paper, but it is critical to note that the implication is that considerable wireless technology sophistication would be required to provide an appropriate design for either a precision jamming system or a MAS implementation.

We are addressing the variability in size by identifying three facility types based on their physical "footprint" (as opposed to inmate population size), those being "large," "medium" and "small." Figure 6 shows specific examples for each of these facility types.

Figure 6. Large, Medium and Small Correctional Facility Working Examples

The large (Federal Correctional Institution in Cumberland, MD) and medium (Dallas County Detention Center) facilities have been previously discussed in Section 2.2. The small facility example is the Anaheim Detention Facility in Anaheim California. Note that both the medium and small facilities are embedded in an urban area while the large facility consists of multiple buildings and open areas surrounded by a security perimeter.

Of course, there are correctional facilities that are smaller than the Anaheim Detention Facility. However, once a facility becomes very small the need for any contraband phone denial system becomes less urgent (i.e., so small that staff can regularly or continually observe prisoner conduct).

4.2 Cost Assessments

4.2.1 Common Elements

Since both Managed Access and precision jamming systems must deliver managed R.F. energy throughout the entire correctional facility (indoors and outdoors), there will be significant similarities between these two systems. These common elements are:

1. **System design and deployment** (Non-Recurring Expense, NRE) that includes site surveys, R.F. propagation analyses, engineering design, and the deployment of the system.
2. **Head-end device(s)** that provides the R.F. interface (Capital Expenditure, CAPEX)
3. **Distribution system** that enables precision delivery of R.F. energy within the correctional facility's perimeter (CAPEX)
4. **Management system** that ensures continuity of service, monitors system/element performance, detects fault conditions and communicates relevant information to the appropriate managers or other stake-holders (CAPEX)
5. **Operational expenses** (Operational Expenditure, OPEX) includes an ongoing assessment of the R.F. footprint. The objective is to minimize and ideally eliminate both unintended coverage holes within the prison facility and leakage beyond the prison boundary. Sensor-based observations are used for incremental propagation modeling / analyses and for fine-tuning adjustments of R.F. coverage (e.g., tweaks to antenna directionality, power levels and other system configurable parameters). Numerous other OPEX costs include management personnel, maintenance, troubleshooting and upgrade activities, among others.

4.2.2 Element Differentiation

Although there are common elements, the specific requirements and associated capabilities of these elements will vary depending on whether it is part of a Managed Access or precision jamming system.

4.2.2.1 System Design and Deployment

4.2.2.1.1 Overview

Each correctional institution has its own unique structure and layout, and in most cases, requires individual surveys, design, engineering, and deployment for the implementation of MAS and precision jamming systems. The R.F. surveys and system designs will need to address factors affecting R.F. propagation including, but not limited to, the footprint of the institution, building materials, internal structures, and locations of inmates. Both system types will require very similar individualized system design and deployment to be effective at denial of service without impacting commercial wireless networks outside the confines of a correctional facility. Given that the intent of the R.F. survey and system designs are similar in nature between MAS and precision jamming systems, there will be very little cost differentiation expected.

MAS and jamming systems should be hardened to withstand damaging weather and other environmental conditions. They should also be hardened against potential sabotage because inmates may attempt to disable the system by destroying infrastructure such as cabling and antennas. The design may require burying cables and erecting fencing around exposed system

infrastructure. These hardening efforts result in cost to the initial design and subsequent operational phase, and will be similar for both MAS and precision jamming systems.

4.2.2.1.2 Relative Cost Estimate

Both MAS and precision jamming systems require similar levels of design and deployment complexity. Thus, due to these essentially identical requirements, the relative cost can be expected to be relatively the same regardless of facility size.

Facility Size	Relative Jamming System Cost
Small	~1x
Medium	~1x
Large	~1x

Table 1. Design and Deployment: Relative Cost for Jamming System with MAS Baseline

4.2.2.2 Head-End Device

4.2.2.2.1 Overview

For a MAS, the head-end device will be a "base station" that provides the bi-directional R.F. communication interfaces. At a minimum, the head-end will need to support multiple cellular bands and technologies (e.g., 2G, 3G and 4G). Most MAS base stations consist of software defined radios (SDRs) that provide simultaneous support for the range of cellular bands and technologies through software implementations on reusable hardware platforms. Through the use of these SDR based "soft modems," various combinations of cellular bands and technologies can be accommodated. The use of SDRs allows the MAS to support multiple cellular bands and generations of technologies/standards in a single system.

For a precision jamming system, the head-end device will be a transmit signal source that provides the service denial interference signal. This interference signal must be highly frequency selective. That is, it must generate energy only in the Down-Link (DL) bands of the FDD systems to be blocked (e.g., cellular) and in the communication bands for the TDD systems to be blocked. All other bands used for legitimate wireless communication must have virtually no significant energy in them. This frequency selectivity is generally implemented using high precision filtering systems.

Given the niche nature of the available correctional facility market, it will be difficult for precision jamming systems to compete with MAS systems. That is, since precision jamming systems will tend to be custom designed solutions for correctional facilities they will have to recoup the costs of engineering, research and development over a relatively small market size. In addition, precision jamming solutions must address the evolving communication landscape (i.e., new generations of mobile access technologies, spanning a more diverse set of frequency bands) within these same niche market constraints.

In contrast, MAS systems benefit from the hardware and software volumes generated by the world-wide, standardized cellular industry. That is, cellular costs are driven by competition among the global ecosystem of vendors and component suppliers, all competing to serve the needs of commercial mobile users. As a consequence, the research and development cost of associated equipment is spread out over a worldwide marketplace and is driven by extremely high levels of competition. Thus, the MAS solutions will be on a steeper cost reduction curve than that of precision jamming.

In comparison, it is difficult to imagine a comparable ecosystem of precision jamming vendors vying to compete based on cost and performance. The vendor ecosystem will very likely be small and limited to proprietary systems with significantly lower market incentive to reduce product costs. This disadvantage will be exacerbated by the introduction of new cellular technologies which will force the proprietary precision jamming systems to evolve within the context of a niche marketplace.

4.2.2.2.2 Relative Cost Estimate

Although the head-end devices used for MAS and precision jamming systems are different in function, the complexity required to implement this functionality is similar. However, as the above discussion demonstrates, MAS head-ends will have cost advantages associated with the volumes and distributed costs of the cellular marketplace. MAS head-ends will evolve to utilize pico-cell technology and leverage their cost reductions over time. Thus, we expect that the precision jamming head-end cost will be at a disadvantage relative to the MAS. The precision jamming disadvantage will likely increase as the facility size increases because multiple head-ends may be required. We have chosen to use conservative estimates for this precision jamming disadvantage pending additional data.

Facility Size	Relative Jamming System Cost
Small	~1.1x
Medium	~1.2x
Large	~1.3x

Table 2. Head-End Device: Relative Cost for Jamming System with MAS Baseline

4.2.2.3 Distribution System

4.2.2.3.1 Overview

MAS systems have been successfully deployed using Distributed Antenna System (DAS) technology. Due to the primary requirement of providing R.F. coverage with power that overwhelms signals from sites outside the correctional facility, an active DAS may be necessary for R.F. signal distribution. An active DAS distributes R.F. signals to active remote units via optical fiber. The remote units require both power and control interfaces.

Since jamming systems need to deliver sufficient interference power throughout the correctional facility to block communication, the R.F. distribution will almost certainly require an active DAS, especially when taking into account the design principles of the local cellular network (see section 3.2.1.3). Each remote unit must interface with an antenna that is capable of covering all channels to be jammed. However, whereas MAS systems require bi-directional R.F. distribution, precision jamming systems require only transmitters on the active DAS. Since active DAS systems up to this point have been designed to improve coverage and performance of conventional mobile services in buildings and venues, they have been designed to be bidirectional. An active DAS system that is optimized for the transmit-only nature of a precision jamming system would require new design and development. Thus, it is assumed that the deployment of a precision jamming system will utilize a conventional active DAS distribution system, with Up-Link signals filtered out at the head-end. Therefore, there is no immediate cost difference that can be garnered from precision jamming systems requiring transmit-only capable active DAS systems.

4.2.2.3.2 Relative Cost Estimate

Both MAS and precision jamming systems are required to cover virtually 100% of the facility area that is accessible to prisoners with signal power greater than that from outside cellular systems. Thus, due to these essentially identical requirements, the relative cost will be virtually the same regardless of facility size.

Facility Size	Relative Jamming System Cost
Small	~1x
Medium	~1x
Large	~1x

Table 3. Distribution System: Relative Cost for Jamming System with MAS Baseline

4.2.2.4 Core Network (MAS Only)

4.2.2.4.1 Overview

The core network provides connectivity and associated features and services from the head-end base station(s) to the commercial wireless network (including the Internet). This network element is required for MAS systems, but is not required for precision jamming systems (since jamming eliminates network traffic). In addition to network connectivity, some MAS vendors use the core network to provide 911 services as well as the lawful intercept and forensics associated with the Communications Assistance for Law Enforcement Act (CALEA). Thus, for instance, under court orders and/or applicable laws, analyses that detail which users are accessing the system including time, duration and frequency, can be provided. Forensics on short message service (SMS) text messages can also be compiled and logged. Some MAS systems also offer services that locate active devices within the facility in addition to managing its communications.

Core networks are nearly fixed price across all sizes of MAS systems. However, the MAS system can support the active phone service, forensics, and overall management based on having the core network connectivity and capability.

4.2.2.4.2 Incremental Cost Estimate

Since a precision jamming system does not require a core network, the cost is an incremental increase for the MAS. Based on discussions with MAS vendors we believe that the MAS core network will add approximately $50K of incremental cost regardless of the facility size.

4.2.2.5 Management System

4.2.2.5.1 Overview

The MAS management system must manage connectivity from the base station to one or more of the commercial cellular networks. It must also provide the monitoring, configuration and user interface capabilities necessary to manage the local R.F. communication system.

The precision jamming management system must also provide monitoring, configuration and user interface capabilities. A reliable, low delay management process is required to ensure that interference issues with nearby wireless systems are quickly identified and resolved.

The MAS and precision jamming management systems will have many common capabilities and functions, including:

- Self-monitoring capability and telemetry features that enable alerting the operator about equipment or component failure leading to signal strength fluctuations (similar cost).
- Signal strength and coverage must be routinely checked to ensure the signal remains within the designed performance parameters inside and outside the correctional facility (expected higher precision jamming cost due to stricter monitoring requirements).
    - The verification of a jamming signal cannot be done remotely unless specific R.F. monitoring devices are installed at multiple locations on the perimeter of the facility. As has been previously noted, R.F. jamming signals must be low enough in power external to the facility so that there is no degradation to the external cellular network. Thus, a monitoring system would need to be installed that continuously monitors the jamming system R.F. power outside of the facility.
    - For a MAS system design, as long as any R.F. signal leakage beyond the correctional facility perimeter is lower in power than that provided by the external cellular network, there will be minimal chance of service degradation to the general public. This condition can be ensured through proper design and deployment of the MAS system.
- The R.F. coverage footprint inside the prison must be routinely checked to ensure the MAS or jammer signal strength is dominant within the facility (similar cost).
- MAS and precision jamming systems may need to be updated to cover new cellular bands and/or systems, resulting in increasing complexity and cost (higher cost for precision jamming expected since the MAS head-end is designed to support efficient upgrade).
- Remote management of all active components for diagnostics and understanding system operational status (higher precision jamming expected cost due to need for higher frequency, lower latency monitoring and response).

4.2.2.5.2 Relative Cost Estimate

Although many of the cost elements are similar between these two systems, we expect precision jamming management costs to be higher for medium and large facilities. This is due to the increasing complexity of indoor/outdoor spaces that must be covered by the jamming signal as the facility size increases, especially if the correctional institute is a campus.

As the facility size increases, there is a corresponding increase in the monitoring and diagnostic capabilities necessary to ensure that nearby wireless systems are not degraded. This issue is of particular sensitivity for jamming systems, as any R.F. energy leakage beyond the facility perimeter can significantly degrade or outright block legitimate wireless communication by the general public. Therefore, the jamming system must be designed to stricter requirements than the MAS, thus increasing the precision jamming system cost. Due to these considerations, the relative management cost for a jamming system is expected to be higher for medium and large facilities.

Facility Size	Relative Jamming System Cost
Small	~1.0x
Medium	~1.1x
Large	~1.2x

Table 4. Management System: Relative Cost for Jamming System with MAS Baseline

4.2.2.6 Operational Expenses

4.2.2.6.1 Overview

This section assumes that a managed and monitored precision jamming management system has been deployed as described in section 4.2.2.5. Given that, then both MAS and precision jamming systems incur common operating expense items that include:

- Costs associated with operational performance testing obligations. The following need to be identified:
    - resources for recurring performance testing (labor and instrumentation for coverage measurement and analysis)
    - operational costs associated with characterization of footprint quality (coverage holes inside and leakage outside the prison facility)
    - testing methodology that will be used to assess the presence of holes and/or leakage
- Management personnel, maintenance and troubleshooting
- System upgrades to accommodate introduction of new technologies and protocols

4.2.2.6.2 Relative Cost Estimate

The costs associated with above functions are expected to be roughly similar regardless of facility size.

Facility Size	Relative Jamming System Cost
Small	~1x
Medium	~1x
Large	~1x

Table 5. Operational Expenses: Relative Cost for Jamming System with MAS Baseline

4.2.3 Cost / Performance Tradeoffs

Given the similar cost associated with deployment of precision jamming and MAS solutions, the question arises concerning cost/performance tradeoffs. For example, if the coverage footprint or operation timespan requirements are reduced, does one of these solutions have an advantage?

Prior to addressing this issue, we reiterate that such requirement reductions will significantly reduce the effectiveness of any solution. That is, given the existence of a highly motivated, adaptable and creative inmate population (with lots of time on their hands), we can expect that even marginal system requirement reductions will be leveraged into major illicit use benefits.

Given this concern, we provide the following assessment for these two systems.

- **System design and deployment** (NRE)

  Both solutions will benefit at similar levels for requirement reductions.

- **Head-end device** (CAPEX)

  This is a fixed cost for both solutions, thus this component is insensitive to requirements reduction.

- **Distribution system** (CAPEX)

  Both solutions will benefit at similar levels for requirement reductions.

- **Core Network** (CAPEX)

  This component is unique to a MAS. The proportional cost impact of this fixed cost will increase as other component costs decrease with requirement reduction.

- **Management system** (CAPEX)

  Both solutions will benefit at similar levels for requirement reductions.

- **Operational expenses** (OPEX)

  Both solutions will benefit at similar levels for requirement reductions.

The above analysis in isolation could be interpreted to suggest that there may be a crossover point at which a precision jamming solution would be more cost effective than a MAS system given the fixed cost of the core network necessary for an MAS solution. However, the numerous additional performance and cost issues previously discussed may suggest that any limited advantage for precision jamming solutions will be more than offset by the many advantages associated with MAS, including long term cost, in the majority of prison deployment scenarios. Most importantly, a reduced-performance "solution" is not recommended because of probable MAS or jamming coverage gaps and thus, it does not address fully the underlying problem.

5 CONCLUSIONS

5.1 Summary

In Section 4 we identified major system elements for MAS and precision jamming systems and analyzed the associated relative cost implications. Three prison facility sizes were considered: small, medium and large (see Section 4.1).

The results (see Section 4.2 for details) are summarized in Table 6. Note that all elements were assessed in relative terms (i.e., cost of the precision jamming system relative to the MAS).

Element	Facility Size Cost Assessment		
	Small	Medium	Large
Design & Deployment (NRE)	~1x	~1x	~1x
Head-End Devices (CAPEX)	~1.1x	~1.2x	~1.3x
Distribution System (CAPEX)	~1x	~1x	~1x
Core Network – MAS Only (CAPEX)	~$-50K	~$-50K	~$-50K
Management System (CAPEX)	~1x	~1.1x	~1.2x
Operational Expenses (OPEX)	~1x	~1x	~1x

Table 6. Cost of Jamming System with Respect to the MAS Baseline

Summaries for the assessed facility sizes follow:

- In a **large** facility, a precision jamming system is expected to be costlier than a MAS system due to larger management and head-end costs.
- In a **medium** facility, the precision jamming system's management and head-end costs are expected to be higher. However, the MAS core network cost would offset some of this difference. Thus, the total cost may be essentially the same, with a possible advantage to the MAS solution.
- In a **small** facility, the additional system cost of the MAS core network will be a larger percentage of the total cost than for a medium or large sized facility. The slightly lower MAS head-end cost will compensate somewhat for the core network cost in this relative comparison. Thus, the MAS may be slightly more costly.

While these results focus on general expectations, because of individual prison characteristics cost variation will occur.

These results are in general agreement with the CellAntenna FCC filing [15] which states that "Managed Access commands only a 10%-15% higher price-tag compared to jamming." Our assessment indicates that a MAS will likely be of equivalent or slightly higher cost for medium to small prison facilities. However, MAS may have a cost advantage in large facilities. Thus, both

we and CellAntenna have concluded that there will be a rough equivalence between the cost of "precision jamming" and MAS solutions.

In addition, Harris Corporation has conducted a jamming vs. MAS assessment that concludes with regard to cost:

> To effectively block calls, the cost, engineering, installation, and logistics of a jamming system are very similar in scope to a managed access system. [16]

The results of this paper are consistent with this analysis.

Because of the extreme diversity in correctional facility characteristics it is impossible to determine absolute cost values. Therefore, we provide the following rough order of magnitude (ROM) ranges of total system cost as a means for calibrating the relative results. Note that these costs assume the above discussed rough equivalence between precision jamming and MAS solutions.

Facility Size	Total Cost Range
Small	$300,000 - $600,000
Medium	$500,000 – $1,200,000
Large	$1,000,000 - $2,000,000

Table 7. ROM Total Cost Ranges (Total = NRE + CAPEX; OPEX excluded)

In Table 8, ROM cost ranges for NRE, OPEX and CAPEX components are provided. These estimates are intended to provide additional context for the relative cost results. The NRE and CAPEX costs focus on the initial system design and deployment. However, over time additional NRE and CAPEX expenditures will be required as the facility evolves and equipment wears out or needs to be upgraded.

Facility Size	NRE	OPEX	CAPEX
Small	$150,000 - $250,000	$30,000 - $50,000 per year	$150,000 - $350,000
Medium	$250,000 - $500,000	$50,000 - $100,000 per year	$250,000 - $700,000
Large	$500,000 - $800,000	$100,000 - $200,000 per year	$500,000 - $1,200,000

Table 8. ROM Decomposed Cost Ranges

Note that the MAS will permit 911 emergency calls, not affect public safety (and other) wireless systems and allow GPS location services. A precision jamming system will likely degrade or disable these critical services. The significant benefits that will be lost by blocking 911 calls using precision jamming systems were discussed in section 3.2.1.2.

Finally, with the deployment of FirstNet, First Responder communications may be carried on commercial cellular bands. Since a jammer does not discriminate between cellular users, first responders attempting to communicate on the affected cellular frequency bands will be blocked. This would be a problem for first responder communications within the correctional facility, as well as outside of the facility if the jammer degrades local commercial wireless networks that also carry First Responder communications.

5.2 Conclusion

Given the significant baseline similarities between MAS and precision jamming systems and the fact that each has marginal cost advantages in specific areas, we conclude that the overall costs will

be similar between the two systems. Operationally however there is an enormous difference in that a jamming system, even if very well designed and skillfully deployed, is still effectively a very "blunt instrument" approach to the problem while the MAS approach is more of a "versatile tool" that has numerous other diagnostic benefits. The MAS solution thus enables prison officials to gain a valuable perspective on the wireless activity in the prison and to use this information as appropriate to detect and deter not only wireless misuse, but potentially other contraband and general criminal activities.

6 REFERENCES

[1] Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, to Devon Brown, Director, District of Columbia Department of Corrections, DA 09-354, February 18, 2009.

[2] "Mobile signal jammers don't work on 3G, 4G in Punjab jails | punjab | Hindustan Times," http://www.hindustantimes.com/punjab/in-punjab-jails-mobile-signal-j…don-t-work-on-high-speed-networks/story-VTrcrIgAvgTVIpYQoA4lBJ.html.

[3] "Analysis of Managed Access Technology in an Urban Deployment: Baltimore City Jail Complex," Engility Corporation, September 2015.

[4] Letter from National District Attorneys Association to Ajit Pai, Chairman, Federal Communications Commission, October 27, 2017.

[5] Letter from U.S. Department of Justice to Marlene H. Dortch, Secretary, Federal Communications Commission, GN Docket 13-111, August 28, 2017.

[6] Letter from Arkansas Board of Corrections to Ajit Pai, Chairman, Federal Communications Commission, GN Docket 13-111, July 20, 2017.

[7] FCC 4th Report and Order, Wireless E911 Location Accuracy Requirements, PS Docket 7-114, Feb. 3, 2015.

[8] Federal Register Vol. 75, No. 91, Wednesday, May 12, 2010, Notices: Department of Commerce, National Telecommunications and Information Administration, Docket No. 100504212–0212–01, Preventing Contraband Cell Phone Use in Prisons.

[9] "Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions," Department of Commerce Report, December 2010.

[10] "Emission Measurement Results for a Cellular and PCS Signal-Jamming Transmitter," Department of Commerce, NTIA Report TR-10-465, February 2010.

[11] "Emission Measurements of a Cellular and PCS Jammer at a Prison Facility," Department of Commerce, NTIA Report TR-10-466, May 2010.

[12] "Initial Assessment of the Potential Impact from a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers," Department of Commerce, NTIA Technical Memorandum 10-468, May 2010.

[13] "Common position proposal on signal inhibitors (jammers) in Latin America," GSMA, 14 July 2014.

[14] "Jails will FINALLY start jamming lags' smuggled mobiles as rollout for high-tech blockers begins." https://www.thesun.co.uk/news/1956860/government-plans-smuggled-mobile-crackdown-in-prisons/.

[15] Reply Comments of CellAntenna Corporation, Howard Melamed, President Jamming Versus Managed Access and IMSI Catching, GN-Docket No. 13-111, 28 December 2017.

[16] https://www.harris.com/sites/default/files/downloads/solutions/mas_vs._jamming_infographic_final.pdf.