Tecore networks

MANAGED ACCESS

CONTROL OF WIRELESS COMMUNICATIONS FOR CORRECTIONAL INSTITUTIONS

CONTENTS

Table of contents

03 ∘ Overview

05 ∘ Managed Access 101

07 ∘ The Tecore Solution

08 ∘ iNAC Success Elements

10 ∘ Patented Technology

11 ∘ Not All Are Created Equal

12 ∘ Competing Technologies

15 ∘ Summary

16 ∘ References

Managed Access

CONTROL OF WIRELESS COMMUNICATIONS FOR CORRECTIONAL INSTITUTIONS

OVERVIEW

As the wireless industry positions for the fifth generation of technology, society is more connected than ever. Over the past ten years the paradigm shift brought about by smartphones and ubiquitous connectivity has driven the buildout of numerous nationwide networks with ever increasing bandwidth driving usage and applications. Coverage and constant availability of services is now part of the fabric of everyday life. However, despite these dynamic changes, there remain isolated situations where wireless services must be controlled. In matters of national defense, public safety, as well as in prisons and jails, communications must be limited to authorized users in order to maintain the appropriate level of security.

As AT&T™, Verizon, T-Mobile and Sprint™ built out multiple generations of wireless coverage throughout the United States, they did so with a license requirement from the Federal Communications Commission (FCC) to provide coverage to a high percentage of the population and land mass. Failure to reach these metrics would be a failure to meet the requirements of the license granted. However these licenses were granted without a caveat or clause for restricting coverage in areas where additional security and control is required. While building their networks to maintain compliance with the FCC, the wireless carriers have inadvertently provided coverage to nearly every prison and jail from coast to coast.

In today's prisons, jails and correctional institutions, this oversight in the licensing process has produced a scenario where many inmates are getting five bars, behind bars, as a by-product. Forty years ago, when the first generation of commercial wireless technologies were deployed, the issue of an inmate with a cell phone was not even on the radar. Cell phones were the size of bricks, coverage was limited and so were the services provided. Today, the severity of the contraband cellular device issue is established as the number one contraband issue in corrections. Inmates are using the convenience and privacy of wireless communications illegally, leading to unmonitored inmate communications and an increased security risk for corrections officers and the general public. Within the walls of correctional institutions, illegal communications from smart phones, tablets, and cellular devices must be controlled, and in many situations eliminated. The challenge posed by controlling communications is the delicate balance between managing coverage throughout the facility without impacting the commercial networks that exists on the other side of the wall, in many cases just feet away.

"Always on" connectivity for inmates is a serious risk. Those with bad intentions and the means of connectivity jeopardize operations within the institution and pose a threat to safety outside the walls in everyday society. While not all communications are for illegal activity, the protection of the personnel in the institution as well as the general public's safety must take precedence. For too long correctional institutions have taken a reactive approach with controlling illegal communications inside the institution; it has been easier to hope nothing happens than to proactively address the issue. With previous solutions addressing only the symptoms of illegal communications,

officers were forced to accept that they cannot address the root cause of the problem. In this scenario they can never catch up or gain control. With Managed Access, the notion that an effective technology solution does not exist is no longer a valid assessment of the situation. In areas where security and communications are of the highest priority, methods are implemented to limit access to only approved users. To accomplish this, mechanisms and controls must be provided to limit and deter unwanted and unlawful communications. Balancing the overwhelming build out of commercial network capacity with a controlled communications environment is a complex challenge. It requires a solution that provides communications control and a list of countermeasures for each deployed technology and band. Solving this problem is the cornerstone of the technology known as Managed Access. Born out of a cellular based solution, Managed Access delivers the appropriate balance between communications control within the walls of the institution and a harmonized deployment with the surrounding commercial wireless networks. The key to Managed Access is the ability to leverage the same technology as the commercial wireless networks to create a credible countermeasure across the spectrum of wireless technologies deployed. With Managed Access, correctional officers are able to work from a position of control and proactively eliminate the threat caused by contraband cellular devices. By being able to control the illegal communications of the inmates, Managed Access delivers the comprehensive solution required to address the contraband cell phone issue.

TECHNOLOGY – MANAGED ACCESS 101

The concept of Managed Access is actually quite simple. Wireless devices leverage protocols and technologies to exchange information with their commercial networks. Most devices today support a combination of technologies across 2G, 3G and 4G LTE. As a cell phone moves from one area to the next, the device selects the best technology and channel for communication. Information is then exchanged between device and network to provide service to the user. Once a network accepts a device, the device is allowed access and "camps" on the local signal broadcast by the network. Subsequent access to place a call, send a text message, or access the internet is all initiated through communications over this channel. The Managed Access Solution (MAS) works from the same principles. It attracts and provides the device service the same way the commercial network does. When a device enters into the coverage area of the Managed Access network, the device is compelled to communicate as if it were still on the commercial network. Once the device accesses the MAS network, it is determined if the device is a ***known authorized device*** or an ***unknown, contraband device***. Depending on the identification of the device, treatment while on the MAS is as follows:

- For ***unknown, contraband devices*** on the system,any subsequent action is met with denial. While the device still appears to be on the commercial network, access to the actual commercial network is denied.

- For ***authorized devices***, the MAS system redirects them to the actual commercial network allowing these approved devices to continue to maintain access to their commercial service.

Through this basic logic, MAS provides the appropriate balance between control of contraband while permitting approved users to continue to use their device in the same controlled space.

Footprint Control

A key element to a successful MAS deployment is the control of the footprint of the system. As the MAS coexists with the commercial network, a balance of power levels and parameters is required to ensure that the commercial coverage is not impacted outside of the institution. When deployed in an urban environment, the balance requires greater precision to ensure the more densely deployed commercial networks are not impacted. An effective Managed Access Solution should be adaptable to the prison facility, location both urban and rural, and the local commercial network environment. The key to a successful managed access deployment is the ability to deliver an effective solution regardless of the operating environment or location of the facility.

Technology Coverage

Another key to the Managed Access Solution is the coverage of technologies and frequency bands in the given area of the deployment. It is a solution with which effectiveness is based on deploying a countermeasure for each technology an inmate could attempt to use. The elegance of the solution is the operation appears to the device and to the inmate as a standard operating wireless network. In today's complex wireless environment, the flexibility of the Managed Access Solution to adjust not only to today's deployed configurations, but to also migrate in the future as operators evolve and enhance their technology solutions is key to the ongoing success of MAS.

Spectrum Licensing

Since Managed Access technology is required to transmit in order to provide the coverage within the institution, the solution requires access to the licensed spectrum to operate properly. This operation is typically granted through a lease or sub-lease of the target spectrum from the commercial operator. Since wireless operators have paid for the rights to the spectrum for their networks, the process of getting permission to deploy a system that impacts the operation of their network would be impossible in most cases. However, wireless operators recognize the significance of the contraband cell phone issue and for this unique case have cleared a path to provide a sublease of their spectrum for the targeted use of Managed Access. Additionally, the process put in place and pioneered by Tecore Networks is one that is currently being followed in the industry and was further endorsed with additional rules put in place by the FCC in early 2017. In its recent Report and Order, the FCC followed Tecore's initial process when defining the rules and regulations to support the licensing of spectrum to Managed Access deployments. Recognizing that the access to spectrum is a key part of the solution, the FCC has implemented rules that require wireless operators to work with Managed Access providers to gain reasonable access to the spectrum for operations. Understanding that spectrum was an impediment in many cases, the rules put in place provide a clear path to spectrum access for the correctional institution and remove one of the major hurdles in deploying managed access.[1]

THE TECORE SOLUTION

The Tecore MAS Solution, branded as the Intelligent Network Access Controller, or iNAC™, is the industry leader in Managed Access technology. As the only system with the proven track record of deployed success and technology evolution, iNAC stands as the only Managed Access solution that has withstood the test of time and proven its evolution capability.

Comprehensive Technology

The iNAC technology establishes a radio frequency (RF) umbrella within a precisely defined target area. Prior to each deployment, a site survey is conducted to optimize the design and configuration of the system. The borders of the target area, as well as the technologies and frequency bands of the local commercial network operators, are taken into account. Tecore's patented technology optimizes its footprint through the use of power control, antenna design, and sophisticated repeaters to limit the coverage of restricted areas to the building(s) or coverage area. The RF umbrella operates in coordination with the local commercial operators who have deployed networks in the area. Coverage of the iNAC System can be tailored for wide open rural spaces or limited to a precise footprint within a building or campus.

Once installed and operational, the devices controlled within the target area will home to the iNAC signal. Based on policies selected by the system administrator, there are two processes for devices:

1. Prohibited devices are locked to the iNAC system and the connection to the outside commercial network is severed.
2. Access requests from approved devices are redirected to the applicable commercial networks after the device is cleared for communications. Users experience no delay in services due to the system's quick turnover.

While locked onto the iNAC system, the display of an unapproved device appears as though it were operating on its commercial network. If the subscriber never uses the device while in the target area, they would not realize the iNAC is in operation. When the user of an unauthorized device attempts to communicate, the iNAC system blocks the effort. Optionally, the iNAC supports enhanced location technology, providing the added benefit of locating the device within the facility in addition to managing its communications. Once the device leaves the iNAC coverage area, it returns to the corresponding commercial network. Unlike other approaches, unauthorized devices under the control of iNAC remain nonfunctional, whether or not it is ever confiscated.

iNAC Managed Access Success Elements

Technology Coverage

The iNAC manages the current technologies deployed by the wireless industry. As 2G and 3G give way to an LTE and WiFi centric world, the MAS must support the full scope of technologies and combinations. The Software Defined Radio (SDR) architecture of the iNAC delivers the flexibility required for this transition. The iNAC system is the only proven Managed Access Solution in the market that has evolved through 2G, 3G, 4G, and now WiFi and 5G. The software defined radio architecture and flexibility of the power amplification system has allowed continued support, while the surrounding commercial wireless technology evolves. Even as new networks and technologies, such as LTE Carrier Aggregation (LTE-A), 600 MHz, 3.5 GHz and WiFi/LTE coexistence lurk on the horizon, the iNAC system is ready to support.

Spectrum Band Coverage

The iNAC supports the current bands where wireless technologies are deployed. Maintaining support for the entire deployed spectum is an ongoing challenge that requires system infrastructure that is prepared for the future. What was three or four bands in commercial wireless just ten years ago, can easily be eight to ten bands today across a wider range of spectrum

Upgradability

While the iNAC addresses the two listed items above, the baseline architecture is also flexible enough to anticipate the changes coming in the future that can impact the deployed infrastructure. With the reality of 5G and the Internet of Things (IoT) , being able to adapt the solution to the changing landscape of wireless is key for continued success of a MAS deployment

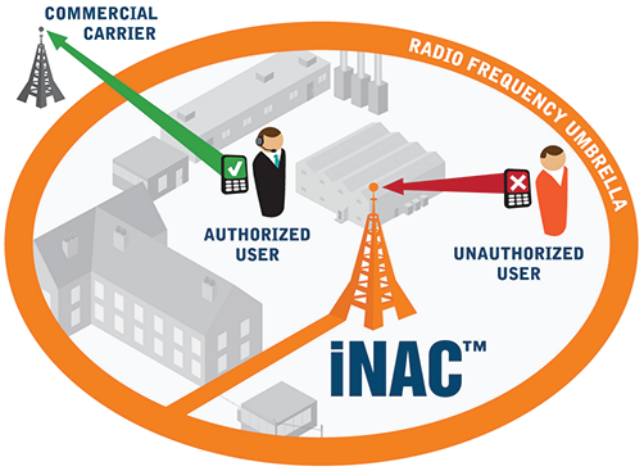
RF Deployment Flexibility

In the corrections industry, no two facilities look alike which can impact the methods and equipment set required to create the proper RF footprint for the institution. Additionally, the surrounding area can also impact the required equipment set based on the required level of control of the MAS signals to obtain the proper balance with the commercial networks outside the wall. iNAC is the proven Managed Access solution when considering successful deployments in various, challenging operational environments.

Emergency Access and Law Enforcement Support

While the basic MAS technology concept provides a basic decision mechanism of approved or an unapproved device, there are unique cases where exceptions need to be made. For example, in many locations in the U.S. and around the world, the system must support an override capability for emergency calls (911 or 112). In this case regardless of the device's status, the call is allowed to complete. This support provides compliance in areas where blocking of emergency calls is illegal or otherwise prohibited

Additionally, the iNAC supports the Communications Assistance for Law Enforcement Act (CALEA) for lawful intercept in accordance with court orders or applicable laws. As subscribers access the iNAC, reports can be captured and generated for each instance. The reports provide an organized analysis that details which users are accessing the system, including the time, duration, and frequency of calls. This reporting option offers important analytical tools for law enforcement and can be enabled or customized to match local laws and regulations.



Installation Flexibility

The iNAC has been installed in urban, as well as rural facilities. While the core technology remains the same, the architecture of the infrastructure required to build the appropriate RF umbrella is significantly different.

Indoor Antenna System

The distribution of RF energy indoors for small to large coverage areas can be resolved by deploying a fiber based distributed antenna system (DAS). The DAS is coupled with Tecore's Multi-Radio Access Network units (MRANs) to provide the required RF signal levels. The signals are then distributed by multiple antennas throughout the coverage areas. Specific locations of the antennas and the appropriate levels of RF energy within any coverage area are determined based on the site survey and RF analysis of the intended coverage area.

Outdoor Antenna System

Outdoor solutions are applicable for larger facilities or coverage areas. This type of deployment operates at a higher RF power and can utilize existing structures. Outdoor antenna systems can provide iNAC with coverage for miles while maintaining the precision control of the service within the targeted area.

Patented Technology

The Tecore Networks iNAC Managed Access is based on a solid foundation of patented technology. The following list of patents outline the targeted capability of the Managed Access solution.

The solution leverages Multi-Technology wireless support, as well as the methods of access control outlined in the nine specific Managed Access related patents.

Patent No.	Name
6,912,230	Multi-protocol Wireless Communication Apparatus and Method
7,733,901	Multi-protocol Wireless Communication Apparatus and Method
8,254,886	Intelligent Network Access Control and Method
8,437,741	Intelligent Network Access Control and Method
8,509,740	Intelligent Network Access Control and Method
8,825,011	Intelligent Network Access Control
9,295,071	Intelligent Network Access Control and Method
9,332,412	Intelligent Network Access Control
9,526,021	Intelligent Network Access Control and Method
9,712,539	Intelligent Network Access Control
9,712,540	Intelligent Network Access Control and Method

NOT ALL "MANAGED ACCESS" SOLUTIONS ARE CREATED EQUAL

As a testament to the severity of the contraband cell phone issue, numerous systems have been introduced touting the managed access capability. Driven by the successful introduction of Tecore's Managed Access in 2008 at the Anexo Guayama, deployedin partnership with the Department of Correction and Rehabilitation of Puerto Rico, numerous other systems appeared in the market. The documented success of the system soon after its deployment grabbed headlines across the corrections industry and provided hope that a long term solution for the contraband cell phone issue had been found.However as time has shown, the copycat approach has not measured up over the test of time and technology evolution.

Technology Challenges

Following this deployment, others in the industry looked to deploy similar solutions. While Tecore's iNAC MAS continued its market leading performance, other less comprehensive solutions faced significant challenges meeting the ongoing evolution of the wireless industry. As the iPhone took hold of the market, broadband data of the 3rd generation became an immediate requirement followed soon thereafter by nationwide LTE deployments. Many of the systems deployed did not have the technical foresight, nor the foundation of capabilities to support this transition. Only the iNAC Managed Access solution has stood the test of time and provided the technology transition roadmap that remains current with the pace of the wireless industry.

Unfortunately several states deployed alternate solutions and have been forced to replace equipment after experimenting with solutions operating under the guise of "managed access". One of the largest states on the West Coast, which once looked to be the leader in addressing the cell phone issue head on, deployed a solution that was unable to upgrade with the technological changes of the wireless industry. After an initial spike of success, the state could only watch as inmates discovered the technology loopholes in the solution as networks transitioned to LTE and deployed in frequency bands not covered by the installed equipment. Almost overnight, the investment made in a static solution, not capable of evolving, was rendered ineffective. Vendors who built their solution based on the assumption that wireless technology was a fixed target quickly failed in the market.

As time has progressed and numerous new commercial wireless networks and bands have been introduced, the initial systems deployed as competition to the iNAC ran short on their ability to accommodate network evolution. The competing MAS's deployed did not have the architectural framework to keep up technically or economically with the pace of change in the commercial networks.

Competing Technologies

Managed Access is not alone in the solutions to defeat contraband wireless communications. There are a number of competing solutions in the marketplace. Alternate technologies of varying sophistication continue to be introduced as the contraband issue continues to be prevalent in institutions around the world.

Traditional Search and Seizure

The most common attempt to defeat contraband wireless is the use of search and seizure in the institution. Through periodic searches, contraband devices are confiscated. Numerous scanning devices are available to help identify the presence of these electronics. These solutions have varying degrees of success and only handle the identification and removal of the devices when and if they are found. Having the inmate population pass within three feet of a metal detector or periodic random searches are staff intensive and only address a small portion of the issue. In addition to this being a marginally effective approach, it is by far the most dangerous solution for the corrections officers and prison guards who work amongst the prison population on a daily basis. Scanning and manual cell phone detection does nothing to disrupt or prevent the communications that took place while the inmate had the device in their possession. This is a solution that chases a symptom of the problem without effectively eliminating the threat. Managed Access exists to remove the reactive measures of scanning and burden on correctional staff.

Detection / IMSI Catching

The concept of Detection/IMSI Catching is that a apparatus is deployed that compels devices to lock to a local signal broadcast by the solution for the purpose of exchanging messaging to obtain the identification information for the user. By capturing this information over a period of time, a list of IMSIs present in the institution is inferred by signal footprint of the detection device and the repetitive access to its signal. The concept is a device that is repeatedly attracted to the IMSI Catcher must be within a certain number of feet from the system, and therefore within the institution. When collected over a period of time a pattern is built to infer that the device must be contraband. While detection “IMSI catching” solutions can identify the relative number of devices in a given area, simply knowing that a device is in an institution is a passive approach and provides no deterrence to the ongoing communications until the device is confiscated or disabled.

Additionally, detection systems that produce lists of devices that meet a certain criteria for being “inside” do not prevent the communications from the device, until the SIM/USIM and device is disabled by the commercial operator. And while this may sound like a viable solution to have network operators disable devices based on an IMSI identifier, the implementation of such an approach becomes unmanageable. While one can contemplate the larger nationwide networks agreeing to disable IMSIs belonging to their network, this approach must also include ALL regional and local wireless operators across the country. This approach will ultimately need to extend to all operators around the world with roaming agreements with US based operators, as each operator

only controls its own subscribers, and not those of national or international roaming partners. So, detection is a short term solution with a number of issues in implementation that will render it ineffective. Much like the requirement of the Managed Access Solution to cover frequency bands and technologies to provide a comprehensive approach, for Detection (IMSI Catching) to be an effective deterrent, all operators must be full participants including those located internationally.

One last point on the detection solutions is that these solutions transmit within the carrier's spectrum. While this transmission may only be for a short period of time and the solution may only hold a device for a few seconds, the fact remains that they transmit in the spectrum in order to collect information from the device. As such, detection solutions that transmit to compel a device to their signal must pursue the same spectrum subleasing agreements required for the managed access operations to remain compliant with FCC regulations. While detection or IMSI catching is proposed by some as an answer to the contraband issue, this does not align with providing a proactive solution to the problem. Much like the search and seizure approach, the Detection/IMSI Catching is reacting to contraband cell phones, not providing a cure.

Beacon Based Technology

Over the past decade numerous technologies have been introduced to provide a solution to handle the contraband cell phone issue. One by one these solutions have proven to be ineffective. The latest technology to gain favor in the market is referred to as "beaconing". The basic concept is a device that hears a beacon within an institution is disabled from operation based on embedded firmware flashed to the device by the wireless operators. This solution is only effective if the custom firmware is successfully installed (and not tampered with, disabled, or bypassed). To be successful, every device on every network must have the firmware embedded. Devices that are not compatible or are engineered to work around the firmware are not impacted by the beacon. To understand how this approach can be rendered ineffective, one only needs to consider that device based solutions will be hacked and can be defeated as they have always been in wireless. There is a reason that the ultimate control and authentication exists within the network itself. Historically device based solutions are not effective once they are compromised. For the same reason that the authentication mechanisms for access to the wireless networks have evolved with each generation of technology. Likewise all it takes is a single hacker to configure a bypass mechanism for the firmware and beaconing is no longer an effective solution. While in theory the application of custom firmware is one approach that is proactive to prevent the communications, it is not practical in its application due to the method of implementation.

Jamming

As long as there are illegal wireless devices in correctional institutions, there will be calls for jamming. This remains illegal in the United States[2] and a cursory glance at this option reveals the significant collateral damage that can be caused by a jamming solution. In the FCC records, there are numerous cases of personal jamming devices disabling a variety of public and commercial communications systems with far-reaching effects. Jason. R. Humphreys of Seffner, Florida was fined $48,000 in April 2014

after an investigation concluded his illegal use of a jamming device "caused actual interference to cellular service along a significant portion of Interstate 4 and disrupted police and other emergency communications" for up to two years.[3] According to the FCC Enforcement Advisory of October 2012, "using or importing jammers is illegal" within the United States. It is also illegal to "sell or advertise jammers online or in stores."[4] In 2016, Chinese Company C.T.S. Technology Co., Limited was penalized by the FCC for "marketing 285 models of signal jamming devices to U.S. consumers via its Aiswa.com website" and selling several devices to undercover FCC personnel.5When deployed in a correctional institution, there exists a similar type of collateral impact on the very commercial communications it is trying to coexist with. The noise introduced into the commercial signals to jam devices is disruptive across all communications within the band. Besides the introduction of noise across the frequency spectrum, Jamming eliminates the ability to process emergency calls or support authorized calls, which significantly reduces the safety and security of correctional staff.

In today's world, the investigative information collected can make the difference in a successful prosecution and in many cases prevent crimes before they happen. One of the main deficiencies of a jamming solution is that through its operation jamming prevents the collection of critical analytics and information about the devices being used and the communications being attempted. This suppression of investigative capabilities eliminates key evidentiary information that could otherwise be collected if a Managed Access solution was in place. Additionally, the sledgehammer method of jamming blocks ALL communications and does not allow the support of critical CALEA capabilities for targeted investigative actions. In both of these cases, Managed Access provides a superior solution as it can collect information from blocked devices to assist investigative efforts as well as support the communication requirements for CALEA.

There are those who point to a significant cost differential between Jamming and Managed Access. The truth of this matter is that both solutions broadcast a targeted footprint of RF technology. To control this footprint requires the deployment of the appropriate complement of signal distribution equipment and capability to create the contoured coverage within the facility. Additionally, a targeted jamming solution requires highly filtered RF signals to properly jam only the intended recipient frequency and technology. This must then be deployed across all frequency bands and technologies available at the facility. The truth is once all of these items are factored into a jamming solution, there is very little difference in the costs to deploy a more comprehensive Managed Access capability.

Jamming remains illegal in the United States and is a solution vehemently opposed by FCC Commissioner Michael O'Rielly, who made a statement in the March 2017 hearing that "no matter how this proceeding moves forward, [he] will not support or approve of any form of jamming technologies."[6] Despite these laws and objections, there are those who continue to advocate for jamming as a technology solution to the contraband issue. What most of these supporters realize is the fact that deploying a selective jamming solution in a correctional institution would be within the same cost structure as deploying a Managed Access solution.

SUMMARY

The issue of contraband cell phones continues to be at the forefront of issues being faced on a daily basis in today's prisons and correctional institutions. For over ten years, the industry has sought to find a comprehensive solution for controlling these communications. While others have provided limited solutions and antiquated approaches, Tecore's iNAC Managed Access solution is the only viable technology that has delivered an effective solution that has stood the test of time.

CONTACT

TECORE NETWORKS
7030 HI TECH DRIVE
HANOVER, MARYLAND 21076

SALES@TECORE.COM
+1 410.872.6500

WWW.TECORE.COM

REFERENCES

1. Federal Communications Commission.GN Docket 13-111. (2017, March 23). https://www.fcc.gov/contraband-wireless-devices

2. Federal Communications Commission. Communications Act of 1934. (1934, June 19). https://www.fcc.gov/reports

3. Federal Communicataions Commission. Forfeiture Order. (2016, May 25). https://transition.fcc.gov/eb/Orders/2016/FCC-16-66A1.html

4. Federal Communications Commission. FCC Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices. (2012, October 15). https://apps.fcc.gov/edocs_public/attachmatch/DA-12-1642A1.pdf

5. Federal Communications Commission. FCC Forfeiture Order. (2016, May 25). https://transition.fcc.gov/eb/Orders/2016/FCC-16-67A1.html

6. Statement of Commissioner Michael O'Rielly. (2017, March 23). https://www.fcc.gov/contraband-wireless-devices


Tecore
networks