WRITTEN TESTIMONY OF DAN WIGGER
Vice President and Managing Director, CellBlox
Before Field Hearing Held by FCC Commissioner Ajit Pai on Contraband Cellphones
Panel #2 – Solutions
Columbia, South Carolina
April 6, 2016

INTRODUCTION

My name is Dan Wigger, and I am the Vice President and Managing Director at CellBlox. CellBlox is a company focused on providing managed access as a service to the US correctional market. We are an innovation leader in applying managed access technology to the contraband cellphone challenge faced by prisons and jails. CellBlox started in Huntsville, AL in 2011, with a focus on developing technologically advanced systems capable of controlling access to commercial cellular networks. The company quickly dedicated its focus to managed access solutions that could be implemented in correctional facilities. Over the years, the company has invested tens of millions of dollars in technologies, partnerships, and in building an organization that supports this managed access mission. As of today, CellBlox has successfully designed, implemented, and now operates multiple managed access systems that have been accepted by a major State Department of Corrections and believe we are the only company that can claim that distinction. CellBlox managed access systems are in service and effectively addressing the challenge of contraband cellphones. Our systems have made an impact on what was previously unrestricted and autonomous use of contraband cellphones from within a prison environment.

CONTRABAND CELLPHONES – MANAGED ACCESS SYSTEM vs ALTERNATIVES

It is well known that contraband cellphones are used by inmates to originate and receive unsecured voice and data communications within US correctional facilities. These contraband cellphones are also used to access the Internet, which results in the public viewing of disturbing comments, pictures, and videos. All of this contributes to uncontrolled communications by inmates that enable the ongoing facilitation of criminal activities such as fraud and extortion, and, allow for tactics that can be used to threaten and harm other inmates, correctional staff, attorneys, judges, and criminal witnesses. This increasing concern for public safety needs resolution.

The problem requires a cooperative solution. We believe managed access provides the solution that can support the correctional market in applying technology that accommodates the needs of all stakeholders. This includes commercial mobile carriers who are licensees of the spectrum that managed access operators must lease, correctional facility agencies and staff, and the public. Managed access, implemented and managed correctly, requires little intervention from local correctional staff resources. Managed access should simply operate and do its job. Alternative approaches to addressing the contraband cellphone problem include detection and jamming, which we believe are less effective and contain additional stakeholder costs in areas that most do not consider. What we do works well – and other less elegant approaches do not work.

Detection. With a detection strategy alone, electronic information from contraband phones can be discovered, and, the approach may also provide the general location of a contraband cellphone device. In our discussions with correctional agencies, we have heard that large detection sweeps can be difficult to orchestrate. Detection methods are hard to conceal, and, many times contraband cellphones often get powered down (off) in advance of the detection exercise and do not get discovered. In addition, even if contraband phones are detected and then directionally located, the next step requires search and confiscation which comes at a risk and cost to the correctional facility staff. Correctional resources must be assigned to physically locate the contraband cellphone which by nature places correctional officers in contentious situations. Furthermore, even if contraband cellphones are only detected and then reported as contraband, and requests are made to terminate service by the commercial mobile carrier networks (for example, ATT, Verizon Wireless), there will always be a high probability that illegal contraband cellphones get reintroduced and the cycle begins all over again. This is resource intensive by those involved, by the correctional facility, investigative staff, and commercial mobile carriers. It should also be noted that if commercial carriers are requested to terminate services based on detection, how long will it take to impact a legal cellphone user's service due to errors made in reviewing and approving detection device results? Resources must also be dedicated to customer service and management. Finally, this strategy also requires development work and continuous processing and administration by many stakeholders involved.

Jamming. With respect to cellular signal jamming, how are jamming systems capable of covering just the target coverage areas? How do they control jamming signals to not "leak" beyond the "intended" area of coverage? It seems jamming as an approach adds further challenges to public safety and does not align with the objective of providing ubiquitous access to 911 services from wireless users to reach emergency responders. Jammed signals present risk by impacting commercial mobile network access on nearby public roads and adjacent commercial or residential areas. There are also the legal issues which the Commission itself has recognized.

These are the hidden costs of these alternative solutions, added administration, added complex processes, and the potential of adding unnecessary public safety risk. With managed access, costs are minimized or avoided. Managed access is designed to identify and control contraband cellphones on a continual operating basis, doing the job of not only detecting, but managing, controlling, and evaluating the environment of contraband cellphone usage. With managed access, the system also facilitates the objectives of providing for limited authorized cellular phone use within a prison property area and is designed to provide access to 911 emergency services should a public cellphone user get connected to the managed access system.

CELLBLOX MANAGED ACCESS IN DEPLOYMENT

CellBlox currently operates and manages multiple managed access systems in the State of Georgia. We provide managed access as a service. We have partnered with the Georgia Department of Corrections at several state prisons. CellBlox is also in the process of implementing additional managed access sites, three in Florida and one in Louisiana, all of which will be completed in 2016. We remain active responding to managed access Requests for Proposals (RFP's), providing industry awareness and

education around our managed access solution, and fielding a large number of managed access inquiries from the correctional market.

In our meetings with Department of Corrections leadership and discussing what their number one contraband cellphone objective is, we routinely receive a response of "just make contraband cellphones useless, make them a brick." CellBlox managed access meets this fundamental requirement of the correctional market without correctional resource burdens. Our deployed solution is in production and blocks contraband cellphone access to multi-carrier, multi-band, and multi-channel commercial cellular services. This includes blocking contraband cellphone access to all of the commercially available US cellular Radio Access Network (RAN) technologies, commonly known as 2G, 3G, and 4G, or, sometimes referred to as GSM, CDMA, UMTS, and LTE networks.

Our most recent managed access installation was completed in Georgia this year. We completed system tuning and installation in February 2016 and received all commercial mobile carrier acceptance and consents in early March 2016. On the first full day of operation, we activated the system at 700AM EST and successfully blocked 938 call and text attempts. This was on the first partial day of operation. On the second day of operation, over 24 hours, a total of 1,915 calls and texts were blocked. Over the first full week of operation, blocked calls and texts totaled 8,952, and for the first 23 days of operation in March, blocked calls and texts totaled 35,705. The data logged by our managed access system also provides information that allows the correctional agency to understand how to improve the security of their facilities by providing blocked attempts by hour of day and technology being used.

CELLBLOX MANAGED ACCESS – TECHNICAL COMPONENTS AND INFRASTRUCTURE

CellBlox managed access utilizes components and infrastructure that are also used by wireless carriers to establish what is known as a Small Cell Network (SCN). As examples, SCN's are installed in enterprise buildings, hospitals, hotels, and in hard to reach underground public transportation stations to enhance commercial carrier cellular coverage in what are difficult to reach indoor building areas. Commercial mobile carriers commonly use what is known as a Distributed Antenna System (DAS) in these environments. CellBlox managed access also utilizes a DAS and uniquely integrates specialized Base Station Transceivers (BTS) with the DAS to create a SCN specifically covering the prison environment.

Key to the foundation of the managed access system is specially developed and proprietary software that integrates all components to replicate the commercial mobile carriers' serving cell sites that provide service to the general area of a prison. Our managed access system then utilizes specific radio protocol messaging (messaging) through the SCN to attract contraband cellphones to capture them and prevent them from reaching the commercial mobile carrier network. Contraband cellphones are then controlled by managed access messaging within the Radio Frequency (RF) coverage area. Messaging is exchanged between the managed access system and the cellphone to identify authorized and unauthorized cellular devices that are in range of the prison coverage area. The system uses its software logic to capture and hold unauthorized devices while allowing authorized devices to be used in

compliance with strict prison cellphone use policies (outbound voice calling only, rejection back to the commercial mobile network, etc.) CellBlox managed access has been further developed to uniquely route 911 calls from within the coverage area (for example, 911 calls can be rerouted to an alternative emergency answer point within the prison), and, to return a voice or text intercept message to unauthorized devices so that the users receive notice that they have been retained by the prison's managed access system. These features can be requested and configured to meet the correctional department's expectations. The managed access system records and stores electronic signature information from unauthorized devices and logs all blocked call and text activities with a date and time stamp. Other information that can be logged is when a device powers on and off, the state of the cellphone (for example, idle vs. active), the number of mobile network access attempts such as initial cell selection or reselection, and number of access attempts by specific radio protocol like GSM, CDMA, UMTS, or LTE.

CellBlox has also developed capabilities that can message to a cellphone that it is stolen, and thus, the device can no longer access any cellular network until it is powered off then back on, and, can target unauthorized devices that abuse 911 dialing by blocking 911 routing from that particular device.

CellBlox managed access is operated and managed "as a service" for the correctional facility. It is remotely accessible and monitored 24/7/365 by CellBlox. As a result, it requires little intervention or management by the agency or local prison staff. It serves to continuously make contraband cellphones useless without needing to confiscate them or report device information to a commercial mobile carrier for service termination. CellBlox managed access includes a customizable User Interface (UI) that provides a dashboard to the correctional agency of the operating status of the system and event logs associated with contraband cellphone activity at a prison. We believe that CellBlox is the only industry provider to offer managed access "as a service" vs. the one-time sale of complicated servers and associated radio and antenna equipment for the agency or prison staff to maintain and operate themselves. We have found correctional departments do not have the resources or expertise to manage these systems, nor do they want to operate these systems. CellBlox also offers financing options to defer and amortize the cost of a managed access system by not requiring a large up-front payment for the entire system, but over time with monthly payments. We are committed to this solution.

MANAGED ACCESS SYSTEMS – RELATION TO COMMERCIAL SYSTEMS

In order to comply with present laws to install and operate managed access, each system must have (a) agreement from the commercial mobile carriers to transmit on their licensed spectrum and (b) approval granted by the FCC.

While managed access functions as a fully independent system isolated from the commercial carrier networks, it is not completely independent of RF signals transmitted by the commercial mobile carriers. Managed access RF distribution must be carefully planned, implemented, and maintained to meet the specific RF environment of a prison's geographic location (urban vs. rural), size (number of inmates and inmate housing unit buildings and their proximity to government-owned property

boundaries), and the number of commercial mobile carriers that provide service in the area of the prison and their associated signal levels. Managed access systems coexist with commercially-provided mobile carrier services and may not interfere with the integrity of commercial mobile networks in publicly-accessible and well-traveled areas. The area of potential interference exists at the RF edge of the managed access system where the RF signal is at parity with that of the commercial mobile carriers. Managed access RF signal levels must be stronger (higher) than commercial mobile network signals within target prison coverage areas and lower (weaker) than commercial mobile network signals in public areas adjacent to the prison. Managed access systems must also consistently cover all bands and channels available from all commercial mobile carriers that service the area of a prison.

MANAGED ACCESS SYSTEMS – IMPLEMENTATION AND OPERATIONAL RECOMMENDATIONS

CellBlox recommends industry cooperation as outlined below.

Managed Access Application Filings and Spectrum Lease Agreements. In order to implement managed access, CellBlox must file with the FCC for a Special Temporary Authorization, or STA, to operate "each" system where spectrum lease agreements between the managed access provider and carriers do not exist. Once FCC approved, a file number and call sign are granted. That information is shared with commercial mobile carriers to facilitate the leasing of their spectrum, including more forms that are filed by the carrier or the managed access provider with the FCC. This is necessary so that we may transmit on their licensed spectrum. To date, commercial mobile carriers have been cooperative in examining the process of granting CellBlox either Spectrum Manager Lease Agreements or Long Term *de facto* Transfer Spectrum Lease Agreements, or, issuing an initial and then ongoing renewed consent letters in order to implement and continue operation of each managed access system. The timelines involved with this process can contribute to longer installations.

We believe through sound regulatory policy, stakeholder cooperation, and common sense, a more streamlined and expeditious FCC and carrier approval process can be achieved. The timeline from initial filing with the FCC to obtaining all commercial mobile carrier spectrum lease agreements and approvals can be reduced. A process that includes agreement by managed access providers that they are bound through a certification process for the specific use of licensed spectrum that complies with the objectives of being a Private Mobile Radio Service (PMRS) provider vs. any right to provide commercial wireless service could expedite managed access deployments.

CellBlox recommends a process where managed access providers can submit certification of their specific use of licensed spectrum, and, utilize a single leasing agreement structure for the leasing of spectrum for the purpose of installing and operating a managed access system.

We support the FCC's recommended process for reducing the time involved with leasing spectrum outlined in its NPRM issued May 1, 2013 in GN Docket No. 13-111.

Managed Access Acceptance Process. Managed access systems need to be accepted by each commercial mobile carrier that provides commercial service in the area of a prison. At present, there is not an industry agreed common approach to system acceptance.

Obtaining a standard process from commercial mobile carriers with respect to required data that must be submitted by managed access providers for acceptance of a managed access system would reduce the timeline associated with installations. Standard items should include testing and acceptance procedures and set timelines to exchange information back and forth. Presently, and depending upon individual requirements from commercial mobile carriers, CellBlox provides an overview of the managed access system, technical specifications of equipment used, capture/release details for each RAN technology to be used, frequency bands and channels to be used, RF containment plans, RF leakage maps, baseline RF signal and final drive test RF scans (comparing the signal strength of the commercial mobile carrier with that of the managed access system), and coordination of initial transmit plans of all managed access utilized frequencies and final commercial mobile carrier testing and acceptance. Each step can take varied amounts of time and there is not a common timeline to process each task. CellBlox understands the necessity of this information for commercial mobile carriers and is committed to implement managed access systems that do not interfere with commercial network performance. The multiple approaches to receive acceptance can and do contribute to lengthier installation intervals.

CellBlox recommends a common intake, application, and review process for the acceptance of managed access systems by commercial mobile carriers. If CellBlox could provide a common set of data points and information that meet reasonable data requirements in order to receive acceptance, the installation interval can be reduced. Specific examples are acceptable RF signal tolerances and acceptance of measured RF signal levels observed from the managed access system vs. the commercial carrier signals immediately adjacent to the prison in public space, but, not on prison or government property.

Through cooperation and agreement, we recommend industry stakeholders strive to reach a common application process, common managed access system information to be submitted, and timelines associated with managed access system deployments between managed access providers and commercial mobile carriers. CellBlox encourages the development of reasonable industry processes so that the implementation interval of managed access systems can be shortened and costs decreased, and do not require direct involvement from any other party (for example, correctional department).

Commercial Mobile Carrier and Managed Access Radio Channel Plan Notice and Change Process. Another area that can improve the installation and efficiency of operating a managed access system is to develop a collaborative working process between commercial mobile carriers and managed access operators that facilitates the sharing of frequency band and channel plans and the timing of commercial mobile carrier network changes. When a managed access system is submitted for review by the commercial mobile carrier, there would be great benefit to receive the current commercial mobile carrier radio plans (band/channel) for the prison area served. This would establish a baseline coverage plan for the managed access provider. Furthermore, when a commercial mobile carrier augments or modifies its wireless network in the area where a managed access system is operational, managed access providers can be “noticed” in advance to plan for and execute changes to the managed access radio coverage plan. Network changes include the addition of cell sites, serving cells, frequency bands, channel changes, capacity mining, and changes of commercial signal power levels. By creating a reasonable “Network Notice Process” between commercial mobile carriers and managed access

providers, modifications could be more efficiently planned and executed. A notice process in this area can also reduce the cost of a managed access system by reducing the costs associated with site visits and eliminate the need to deploy RF scanning equipment at a managed access site that only exists to monitor the commercial mobile carrier environment for changes made. If there were a defined and proactive notification process between carrier and managed access provider, these cost elements could be avoided. CellBlox believes there are similar notice processes in use by carriers today that would not impose any material burdens on the commercial mobile carriers, and, proactive notice would facilitate the objective of a managed access system continuously identifying and controlling cellular contraband in sync with the commercial mobile networks.

Sharing of Key Performance Indicators (KPI) and Network Performance Diagnostics. Commercial mobile carriers are focused on maximizing their service coverage areas and in providing their customers with a superior wireless experience. A managed access provider is focused on providing maximum RF coverage within a prison's high risk buildings to detect the presence of and attract and capture contraband cellphones. CellBlox recommends industry KPI sharing to ensure both objectives can be achieved.

With a managed access system, there will always be an RF "edge", meaning, the open spatial area that the managed access RF signal and the commercial mobile carrier RF signal compete and are at parity. This edge is required to be within, around, or just outside of the secure perimeter fencing of a prison, but still on government prison property. Where this RF edge exists, there will be competition for a cellphone to register and obtain service with either the managed access system or the commercial mobile carrier network. It is at this intersection point that open sharing of network performance data can be utilized by a managed access provider and commercial mobile carrier to pinpoint and understand the location of any network degradation that may be perceived as effecting public access to the commercial network (for example, commercial carrier call drops occurring in a prison yard vs. the public highway). Specifically, managed access RF signal levels can be measured and shared using industry accepted test equipment, and, commercial mobile carrier network performance tools can be equally shared at these precise points to confirm that the presence of a managed access signal does not interfere with public use of the commercial mobile network outside of this RF edge. KPI and network diagnostic tools can also assist in pinpointing the precise locations of any interference concern. As an example, if a commercial mobile carrier sees a degradation of call retainability (high number of forced call terminations, or call drops), sharing of its KPI data and the location of the call drops could quickly determine if the concern is on government land covered by a managed access system, or, beyond the intended coverage area of the prison managed access system.

CellBlox recommends that a process of confidential network KPI and diagnostic sharing would better facilitate detailed understanding between managed access provider and commercial mobile carrier of the KPI changes that result where a managed access system operates in the prison area and on government property. From our experience, example carrier measurement changes include reductions in cellphone access requests, call volumes or traffic, and call retainability. With properly designed managed access systems, this RF edge is not in the public space, but exists on government property and could be easily assessed. CellBlox recommends that commercial mobile carrier networks "carve out"

KPI's associated with submitted managed access coverage areas of a prison property as a managed access system will inevitably have a RF coverage edge and impact these types of carrier metrics at this intersection point.

Finally, working with correctional agency representatives, all stakeholders can cooperatively work on defining agreed-upon areas of what are heavily restricted commercial mobile carrier access on government property by the general public (inmate visitation access areas, vendors access areas, etc.) and correctional staff that align with meeting managed access coverage objectives and stringent security policy. All industry stakeholders can and should agree on what signage can be used at entrance points to a prison to signify that a controlled cellular environment exists and that there is restricted cellular service (for example, 911 only) in those posted areas. CellBlox believes this is a simple and economical notification method to inform the public of the seriousness of controlling contraband cellphones on government property in and around prisons. CellBlox desires to work with the wireless industry and correctional leadership on what should be acceptable use of cellular phones on government property in and around a high security prison that integrates with the objectives of controlling contraband cellphones, managed access deployments, and RF coverage areas.

CONCLUSION

Managed access systems are the most technologically feasible solution to the growing contraband cellphone issue. Managed access as a service requires little management or intervention by correctional staff by simply operating as a 24/7/365 service, monitored remotely, that identifies and controls all contraband cellphones in its targeted coverage area. CellBlox managed access is capable of meeting many stakeholder objectives through advanced technology and a multitude of configuration options. With ongoing and added cooperation between regulatory agencies, commercial mobile carriers, managed access providers, and correctional representatives, managed access can be installed in a more timely manner, and, can coexist with commercial mobile carrier networks and require minimal administration from them. A common application and approval processes, common managed access acceptance processes, and further data sharing between managed access providers and commercial mobile carriers can further reduce cost and implementation timelines for advanced managed access solutions for the correctional market.

CellBlox encourages solutions and policies that involve cooperation of stakeholders vs. solutions that are implemented in isolation and require the commercial mobile carriers to accept solutions that may cause widespread interference and jeopardize public safety initiatives. We firmly believe that cooperation and the furtherance of ideas, worked together, can expand the efficacy of managed access solutions, and meet policy objectives involved with technical solutions that can eliminate contraband cellular use in our nation's prisons. Managed access systems operate effectively and in conjunction with commercial mobile networks today, and can be developed even further with full stakeholder input and cooperation. With managed access, overall public safety will be improved and there is not an introduction of new challenges.

CellBlox looks forward to working with the correctional market, FCC, and commercial mobile carriers to continue to address the challenge of contraband cellphones.

SUMMARY

1) CellBlox is a managed access expert with systems operating and accepted;
2) Managed access is the only technology that meets all constituent needs;
3) Managed access makes inmates, friends and family, corrections, law enforcement, victims, witnesses, and all of society safer.