TESTIMONY OF
MARJORIE K. CONNER, ATTORNEY
AT FCC COMMISSIONER PAI'S FIELD HEARING ON
CONTRABAND WIRELESS DEVICES IN CORRECTIONAL FACILITIES
COLUMBIA, SOUTH CAROLINA
APRIL 6, 2016

Legal Framework for Technological Solutions

In the matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, *Notice of Proposed Rule Making,* GN Docket 13-111, 28 FCC Rcd 6603 (2013) (the "Contraband Wireless Device Proceeding"), the Commission identified the problems arising from contraband wireless devices in correctional facilities.

In the Contraband Wireless Device Proceeding, the Commission sought comment on three technological solutions by which corrections officials might battle contraband wireless devices. Specifically, it sought comment on Managed Access Systems ("MAS"), Detection, and Jamming.

With respect to MAS, the Commission specifically sought comment on a process to immediately grant *de facto* lease agreements or spectrum manager lease agreements for spectrum used exclusively in MAS in correctional facilities, and streamlining other aspects of the lease application or notification review process for those MAS in correctional facilities. It also proposed classifying MAS operating in correctional facilities as private carriers for the purposes of processing special temporary authority ("STA") applications.

With respect to Detection systems, the Commission proposed to require wireless providers to terminate service, if technically feasible, to a contraband wireless device if an authorized correctional facility official notifies the wireless provider of the presence of the wireless device within the correctional facility. The Commission asked for comment on any

limitations imposed on the Detection protocols by Section 705 of the Communications Act of 1934, as amended, 47 U.S.C. §705.

As the Commission considers various technological solutions, as ever, it is mindful of the the limits imposed by the Communications Act of 1934, as amended 47 U.S.C. § 151, *et. seq.* (the "Act"), generally. The Commission must thread the needle of the Act's limitations, while effectively addressing the troubles wrought by continued use of wireless devices by prisoners in correctional facilities in the United States.

The evils wrought by contraband wireless devices in correctional facilities are so vexing that almost every state in the Union has a rule or regulation making wireless devices contraband in correctional facilities. In 2010, the U.S. Congress amended Section 1791 of the Criminal Code, 18 U.S.C. §1791, to clearly make wireless devices contraband in federal prisons.[1] If these devices have been outlawed virtually everywhere, it seems to follow that they would be eradicated. Alas, the problem continues unabated.

Technological solutions are available to eradicate contraband wireless devices in correctional institutions. Because the contraband wireless devices operate on radio signals that can be detected, managed, and even interrupted, the signals may be detected, directed, and even jammed. Each of these strategies is effective in its own way. Each of these strategies is complicated by the Act and the rules, and by carrier cooperation.

I. Jamming

Technology makes management of the spectral environment possible, but Section 333 of the Act limits how corrections officials may manage the environment, even within the

[1] Cell Phone Contraband Act of 2010, Pub. L. 111-225.

boundaries of their own facility. Although blanket jamming is clearly the most effective means of stopping communication, contraband or otherwise, it is made illegal by Section 333 of the Act.

Section 333 says:

> No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government.

47 U.S.C. § 333

Wireless carriers are authorized under Title III of the Act, which is the "chapter" to which Section 333 refers.[2] Wireless devices operating on the carriers' networks are authorized under the carriers' licenses, and so are protected by Section 333. Without forbearance by the Commission or action by the federal legislature, wholesale jamming of signals, even within correctional facilities, is illegal.

II. No-service zones

In a different way, however the Commission might eliminate signals to wireless devices entirely. In the Contraband Wireless Device Proceeding, parties argued that the Commission has authority to modify spectrum licenses to prohibit (or at least not authorize) radio communications in certain specified areas, in effect, creating no-service zones. Parties argued that, in this way, the Commission could solve the problem of contraband wireless device use by making use impossible. If the signal somehow reached a no-service zone, jamming of it would be permitted, as the radio signal is not authorized. In the context of correctional facilities, no-

[2] *See* table of contents of the Act.

service zones may be an effective tool to battle the illegal and dangerous use of wireless devices in correctional facilities.

The European Union has adopted special rules limiting the licensing and operation of mobile services in aircrafts[3]. Specifically, the European Union has found that public safety concerns trump any rights spectrum licensees may have to provide service within the cabin of an airplane. As Boeing explained in its comments in the Contraband Wireless Device Proceeding, "European regulators considering the similarly isolated spectrum environment inside an aircraft cabin concluded that carriers have no expectation of control of spectrum within the cabin of an aircraft and that mobile devices in this unique environment could and must be controlled by the airline." Analogies may be drawn between these unique environments where spectrum must be tightly controlled to ensure the safety of both prisoners and the public.

It seems to follow that each correctional facility should be allowed to determine its need for a "no service" zone. Local decisions relieve the FCC from any sweeping action and allow local conditions to dictate the need. Because each jail or prison faces unique challenges in terms of its geography, jamming may not be appropriate or possible in all areas. For example, while the accuracy of jamming technology has greatly improved, jamming may not still not be appropriate in urban city jails that are located in densely populated communities.[4] Therefore, the FCC should establish a process by which "no service" or quiet zones may be established. For example, the Commission may set up a process by which corrections officials could petition

[3] Comments of Boeing Company, filed July 18, 2013, at 10.
[44] *See* Marcus Spectrum Solution Comments at 21.

the FCC to have the boundaries of their facilities declared a “no service” zone. Any request would be served on each carrier providing service to the proposed "no service" zone. The carriers may have a time in which they can object and then along with the public service and corrections officials, the FCC may make a determination on whether the "no service" zone should be designated.

Once designated, the FCC may establish a process for those providing service outside the “no service” zone to register complaints about interference emanating from within the "no service" zone. Such safeguards would be more than sufficient to meet the concerns of the communities surrounding correctional institutions, while still permitting the use of cell phone jamming within correctional institutions when such measures are appropriate.

Inversely, if service were to bleed into the correctional facility, it might be jammed, without violating Section 333 of the Act.

III. Managed Access

As micro-cellular device, the MAS includes a base station configured to cover a correctional facility, and tuned to operate on the frequency bands of the wireless provider networks. MAS is designed to be the strongest signal within the targeted area, so that any transmission from within the correctional facility attempts to connect with its provider network, it will be processed first by the MAS.

MAS processes each call according to lists created by local corrections officials that identify authorized devices that may operate from within a specific correctional facility. Any other wireless device that attempts to operate within the facility is denied access to its

network. Unauthorized devices are, in effect, jammed, at the discretion of local corrections officials.

Because it operates a micro-cell base station, in order to operate an MAS, a correctional facility must enter into some arrangement with the major carriers. In comments in the Contraband Wireless Devices Proceeding, Tecore noted that negotiations with the major carriers could be challenging. It proposed a "shot clock" or a timetable for negotiations of the lease or other agreement for operation of a MAS. Without a consequence, however, a shot clock is of little value.

Also in the Contraband Wireless Devices Proceeding, the Commission noted that each lease agreement must be approved by the FCC. The FCC has proposed streamlined processes and for the granting the lease applications.

Occasionally, pending approval of a lease agreement, MAS users obtain special temporary authority to operate the systems. The Commission proposed to streamline the STA process, as well, including waiver of the advance filing requirement.

MAS is an expensive technology that must be updated for each evolution of wireless service. When an obsolete MAS cannot interface with the technology, it defaults to a blanket go/no go. It either clears every call or denies every call. Effectively, jamming all calls.

IV. Detect and Deactivate

Detect and deactivate is considered to be like pest control for wireless devices in correctional institutions. In the usual detect and deactivate scenario, occasionally, the detection service sweeps the correctional facility and identifies the devices present in the facility. DAS-integrated detection equipment derives more robust information. That better

information can be passed on to the carriers for more certain suspension of service. To be effective, at a minimum, the detection equipment must identify:

1. IMSI/IMEI for GSM and UMTS devices and ESN/MIN for CDMA devices;

2. Verification that proper functioning of the device was confirmed within seven (7) days immediately preceding the date of the notice;

3. Verification of a confirming search identifying each of the listed contraband devices at least two times within a three (3) day period.

If a wireless device is found in a correctional facility, the corrections official then sends a notice to the carrier serving the device. For ease of processing, a form of notice should be developed to include:

1. IMSI/IMEI or ESN/MIN, the first time it is observed; and

2. The number of times the device is observed in the correctional facility since the first observation

All the detection and reporting in the world is useless without swift carrier action to suspend service to devices detected as contraband on prison premises. In the Contraband Wireless Devices Proceeding, the Commission proposed requiring action by the carriers. Each carrier can bring its own talent and experience to bear in assessing the reports of contraband devices on prison property, but must suspend service unless there is a good reason not to do so.

In the Contraband Wireless Devices proceeding, the Commission proposed a requirement that providing carriers deactivate wireless devices reported as operating illegally in correctional facilities.

V. Concerns about access to 911

NENA, the 9-1-1 Association, AT&T, CTIA, and VANU Cellular Suppression have have raised concerns about bleed over of the combative efforts which may interfere with access to 911 near, but outside the correctional facilities. Not a single incident of 911 blocking from MAS or other combative efforts has been reported. Rather, a rash of problems associated with prisoner access to 911 have been reported

Amusing anecdotes about prisoners calling 911 to report being held against their will or mistreated by prison officials abound.[5] But prisoner access to 911 is no joke. As the Office of the Secretary, State of California - Department of Corrections and rehabilitation noted in its comments:

> When technical difficulties resulted in its MAS being briefly inoperable, inmates were left with the impression that a call to emergency 9-1-1 would result in MAS being inoperable and their cell phones would be usable. The PSAP (an emergency dispatch center in the rural county in which the prison is located) received hundreds of non-emergency calls from inmates attempting to bring down the MAS. … Had any true emergency call come through during the time the dispatcher was tied up on one of the hundreds of [inmate] calls, the results could have been tragic."[6]

This type of harassment is typical.

Allowing contraband wireless devices to dial 911 or any other number is inviting inmates to harass the unfortunate person with the duty to answer the call when it comes. The

[5] Scottsdale Woman Booked for Calling 911 From Inside Jail, June 20, 2012, ; Man Calls 911 From Jail: "I'm Getting Hogtied to the Holding Cell Up Here", March 11, 2011, AOL News, http://www.aolnews.com/2011/03/18/man-calls-911-from-jail-im-getting-hogtied-to-the-holding-cel/; Carly Houston to Naperville 911, "Help, I'm Trapped Inside a Jail," March 24, 2010, The Weekly Vice, http://www.theweeklyvice.com/2010/03/carly-houston-to-naperville-911-help-im.html; Pete Kotz, "Joseph Walsh Calls 911 From Jail to Complain About Being Mistreated," True Crime Report, March 16, 2011, http://www.truecrimereport.com/2011/03/joseph_walsh_calls_911_from_ja.php.

[6] California Corrections at 4.

Commission should not require any of the available technologies to complete calls to 911 from contraband wireless devices.

VI. Solutions

Technological solutions to the problems arising from the use of contraband wireless devices in correctional facilities exist. The Commission holds the power to create no-service zones, to ease the burden on MAS operators, and to order carriers to deactivate the vexing devices. While the Act provides guidance, it does not stop the Commission's efforts to solve the problem.