TESTIMONY OF GERRY KEEGAN, ASSISTANT VICE PRESIDENT

AT FCC COMMISSIONER PAI'S FIELD HEARING ON CONTRABAND CELLPHONES

COLUMBIA, SOUTH CAROLINA

APRIL 6, 2016

Good afternoon. My name is Gerry Keegan with CTIA, the trade association representing the wireless ecosystem. Thank you for the opportunity to testify today regarding potential solutions to the problem of contraband cell phones in our nation's correctional facilities.

On behalf of CTIA and its members, let me be absolutely clear about our overarching interest in this matter: we fully support policymakers' efforts to keep contraband wireless phones out of correctional institutions. Our carriers have no legitimate subscribers residing in these institutions and no interest in seeing inmates use wireless services for any reason. We want to work cooperatively to develop and implement measures that will solve this problem and preserve the ability for law-abiding members of the public to continue to reliably access the wireless services provided by CTIA's member companies.

In this regard, CTIA, working with its members and other participants in the wireless industry, have been actively engaged in developing technologies and services that address this problem while ensuring the continued effectiveness of lawful cell phone use. CTIA, together with its members and numerous other organizations, have been at the forefront of the effort to curb contraband device use. Years before the Federal Communications Commission (FCC) initiated a rulemaking proceeding on this issue, CTIA

and its member companies were actively working with managed access and cell detection technology vendors to: (1) identify approaches that would curb the use of contraband cell phones in prisons; and (2) deploy these solutions in correctional facilities. Specifically, as early as July 2009, CTIA convened a meeting and discussion among vendors of technological solutions (such as managed access) with engineers from a number of CTIA wireless carrier members to discuss potential solutions to contraband devices in correctional facilities.[1] This led directly to CTIA engagement with correctional institutions, such as the Maryland Department of Public Safety and Corrections, to investigate and develop collaborative solutions. Meanwhile, CTIA's carrier members have made their licensed spectrum available for the operation of managed access systems in correctional facilities across the country.

While the wireless industry has worked collaboratively with correctional institutions to address the serious problem of contraband wireless devices in prisons, CTIA stresses that this is ultimately a *contraband* problem, not a telecommunications policy issue. Communications regulation alone will not sufficiently guard against contraband device use. It is for this reason that CTIA strongly supported the Cell Phone Contraband Act, which became law in 2010 and punishes Federal inmates with a wireless device, as well as anyone who supplies them with one. CTIA also supports state legislation to criminalize and increase penalties for the smuggling of cell phones to inmates and the possession of those phones by inmates. More generally, CTIA supports lawful solutions that involve the

[1] Vendors in attendance at the meeting included Airpatrol of Columbia, MD, BINJ Laboratories of Quincy, MA, Electronic Entities Group of Torrance, CA, ITT of Columbia, MD, Tecore Networks of Columbia, MD, CellAntenna of Coral Springs, FL, and Triple Dragon Communications of Vancouver, BC.

collaboration of state and local governments, correctional facilities, software and equipment vendors, and wireless carriers.

I will now discuss four solutions that have been proposed to combat the possession and use of contraband cell phones within correctional facilities. *First*, the wireless industry and corrections facilities have embraced managed access technologies as an effective means of preventing unauthorized wireless communications within prisons. *Second*, a comprehensive review of *how* contraband devices enter corrections facilities will empower stakeholders to develop more effective solutions. *Third*, wireless carriers have expressed a willingness to terminate an identified contraband device upon receipt of an order from a court of relevant jurisdiction. CTIA submits that this should be the *only* condition under which wireless providers are required to take such action. *Fourth,* while jamming has been cited as a means of curbing contraband device use, there are many harmful side effects to the use of jamming technologies, which is why the use of jammers is generally prohibited under Federal law.

Managed Access. Managed access and detection systems have proven highly effective in combating the use of contraband wireless devices in prisons. Managed access systems are micro-cellular, private networks that analyze transmission to and from wireless devices to determine whether the device is authorized to access public carrier networks. Managed access system base stations capture all voice, text, and data communications within the system's coverage area and cross-check the identifying information of the device against a list of authorized devices. If the device is not

authorized, communications are terminated. Meanwhile, users of authorized devices may continue to access public carrier networks as they normally would.

To operate managed access systems, operators of these private networks require a right to transmit over commercial mobile spectrum licensed to commercial wireless carriers. Wireless carriers whose licensed service areas overlap the footprint of state or local corrections facilities work with managed access system providers to arrange for access to spectrum. Once consent is obtained from the carrier, a lease application is filed with the FCC to enable managed access system deployment on the carrier's spectrum. CTIA and others have asked the FCC to put into place streamlined procedures that would permit these lease applications to be processed more quickly and efficiently. CTIA and its members also support liability protection for carriers in the event that a managed access system blocks or degrades a call to 911.

Managed access systems have been deployed throughout the country and are currently used at a number of state and local corrections facilities. The wireless industry favors managed access systems because they block unauthorized communications, reduce incentives for parties to smuggle contraband phones into prisons, and permit lawful communications to take place without interruption or degradation.

Comprehensive Review. To truly combat the use of contraband cell phones in prisons, stakeholders must conduct a comprehensive review of how these devices get into correctional facilities in the first place. This is ultimately a *contraband* problem. While the wireless industry has readily assisted corrections facilities in preventing unauthorized communications from devices already inside prison walls, CTIA and its members believe

additional focus must be given to *preventing* the import of these devices in the first place. By gaining a clear understanding of how these devices get within prison walls, state and local authorities can take targeted action to stop contraband cell phones at prison boundaries. Critically, states must adopt harsh penalties not only for possession of contraband cell phones, but also for supplying inmates with these devices and/or financing the associated wireless service.

In addition, some consideration should be given to the implementation of "airport style" security measures for staff and visitors who enter prison grounds. Remarkably, not all correctional facilities require even the same level of security checks to enter a prison facility that citizens and staff routinely encounter when entering a congressional office building. In facilities that do require "airport style" security measures as a prerequisite to entry, officials "consider this interdiction method effective at curbing cell phone smuggling at the point of entry" and the Federal Bureau of Prisons believes the screening process "has been a good deterrent."[2]

Termination of Service. Several parties have called for wireless carriers to terminate service to devices alleged to be contraband. However, without a proper legal framework governing requests for service interruption, such actions may be legally suspect. Wireless carriers receiving requests to terminate service are faced with a dilemma - they must determine whether there is sufficient proof of unlawful use to justify deactivating the device. Carriers should *not* be charged with determining whether a particular device is contraband. There is a remote possibility that, for example, a cell

[2] Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety, Office of the Inspector General, State of California, May 2009, at 6.

detection system could mistakenly identify a lawful device as contraband. Should a carrier deactivate such a device without further verification, this could endanger the safety of a law-abiding wireless user and expose wireless carriers to significant liability. And, in some cases, full deactivation of a device or a portion of a wireless network simply is not possible. For these reasons, any notice to terminate an identified device must come from a court of relevant jurisdiction. Both wireless carriers and prison officials are familiar with responding to court orders, and this requirement will protect both carriers and their law-abiding customers, while still empowering carriers to take action against unlawful use.

Jamming. In addition to concerns about effects on the public and public safety, the law on wireless jamming is clear: jamming by non-Federal entities constitutes an unlawful interference with radio communications in violation of Section 333 of the Communications Act. Consistent with this law, the FCC has taken swift and forceful action against the users and manufacturers of these unlawful devices. Jamming is also an overly blunt instrument. If a managed access system is a scalpel, a wireless jammer is a sledgehammer. By blocking *all* wireless communications inside and near corrections facilities, legitimate communications are blocked and, if the jammer fails, corrections officials have no further recourse against users of contraband phones. Tests conducted at the Baltimore City Detention Center revealed that jammers blocked wireless signals well outside of prison walls, including on nearby thoroughfares. This creates an extremely dangerous situation for lawful wireless users outside prison walls, who may find a critical call to 911 blocked by a malfunctioning or over-inclusive jammer. Put simply, when

discussing potential solutions to the contraband phone problem, jammers cannot and should not be on the table.

CTIA looks forward to actively participating in the effort to curb contraband cell phone use. I would like to thank Commissioner Pai and the organizers of this field hearing for allowing me, on behalf of CTIA, to present our views on this critical public safety issue.