Testimony of
Steve Largent, President and CEO, CTIA – The Wireless Association®
on Contraband Cell Phones in Correctional Facilities:
Public Safety Impact and the Potential Implications of Jamming
before the Senate Committee on Commerce, Science, and Transportation
July 15, 2009

Thank you for the opportunity to appear before you today on behalf of CTIA – The Wireless Association®.

On behalf of CTIA and its members, let me be absolutely clear from the outset on two points: First, we understand the reason for today's hearing and fully support policymakers' efforts to keep contraband wireless phones out of correctional institutions. Second, our carriers have no legitimate subscribers residing in these institutions and no interest in seeing inmates use wireless services to conduct unlawful activities or harass or intimidate the public. We want to work with the Congress 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.

Resolving this issue in a way that both protects and serves the public will require cooperation among Federal and state policymakers and administrators and industry, and I'm here to pledge the wireless industry's assistance in this effort. That said, it is the wireless industry's view that the jamming of wireless signals is not a panacea and raises potentially serious concerns that must be taken into account as Congress contemplates how to address this issue. While some parties have attempted to position jamming as "the solution" to controlling contraband phones in correctional institutions, we do not believe it should be a preferred solution given the availability of superior technological alternatives.

Foremost among the concerns we have with any jamming proposal is the impact it could have on the ability of wireless service providers to reliably and effectively provide critical connectivity to public safety officers, including first responders who may have to enter a prison to fight a fire or deal with another emergency, and other legitimate customers. The public safety role of commercial wireless services is well known to the American public and members of this Committee. The industry provides access to 911 and E911 services, offers priority access service to government officials in times of natural or man-made emergencies, and is working to bring emergency alert services to market as soon as the Federal Emergency Management Agency (FEMA) releases the standards under which the EAS process will be implemented. Wireless consumers rely on their ability to use their wireless phones as lifelines in time of need and for their daily business and personal needs, and thus the possible authorization of jamming without due regard for the consequences of such a decision and the interference it may cause is of serious concern to CTIA's membership.

Since enactment of the Radio Act, this Committee has played a vital role in shaping wireless policy, and one of the long-standing cornerstones of that policy has been the prevention of willful interference with radio signals. This was reflected in the Communications Act of 1934, and reiterated in the 1990 amendments that added Section 333 to the Act. We believe these sound policies have worked well, and before departing from them we urge policymakers to consider whether there are reasonable, effective, and affordable technological solutions that would better solve the problem. We believe there are and want to highlight several alternative solutions that policymakers should consider.

The first of these alternative solutions is cell detection, a monitoring and tracking approach that allows for the identification of individual wireless devices within a correctional environment. Cell detection does not create interference and thus these

systems can operate without causing problems for legitimate wireless users operating in commercial or public safety bands.

With cell detection systems, prison administrators and correctional officers can detect, locate, and confiscate unauthorized wireless devices found in a correctional environment. Confiscated wireless devices can provider correctional authorities and law enforcement with call records, address information, and even photographs that can assist in disciplinary actions and criminal prosecutions. Alternatively, once illicit devices have been detected, prison officials and law enforcement may decide to leave them in place and arrange to monitor them in accordance with the wiretap statutes. As demonstrated in the recent high-profile case in Baltimore in which a number of inmates and correctional officers were indicted on the basis of information gathered by wiretaps, intelligence gathered in this way can be a critical tool that assists law enforcement in investigations and the prevention of criminal activity.

Cell detection technology is available today, and the United States Department of Justice recently acknowledged the need to improve its ability "to detect, locate, and defeat the use of unauthorized wireless communications devices in all operating environments, including in, but not limited to, correctional environments," adding that it also requires "improved, unobtrusive means to accurately detect a broad spectrum of contraband to preclude its introduction into correctional … environments."[1] These functionalities are not possible with jamming, which may thwart the use of contraband phones in some cases but will not prevent smuggling, identify the location of unauthorized devices, or assist in their confiscation.

In addition to cell detection, another promising technological solution to this problem involves the use of managed access. This approach enables a corrections facility to manage wireless access in controlled area, such as a prison. Managed access would

[1] U.S. Department of Justice, National Institute of Justice, "High-Priority Criminal Justice Technology Needs," March 2009, at 16. Document available at http://www.ncjrs.gov/pdffiles1/nij/225375.pdf..

restrict communications on the commercial wireless networks to only a subset of allowed users (also known as a "white-list"). Other users are blocked from the commercial system access in the area. Managed access solutions also utilize location-determination technologies to ensure that the controls apply only in the geographic area of the prison. And the best part is, because no jamming transmission occurs, there is no interference to other users.

Just last week, CTIA convened a day-long meeting involving North American vendors of cell detection and managed access solutions[2] and engineers from a number of CTIA's carrier members to discuss potential solutions to this issue. We hope our efforts will put the industry in a position to trial alternative solutions in partnership with various states, including the Maryland Department of Public Safety and Corrections, with which we have had an on-going dialogue about ways in which we can collaborate to resolve these issues in a way that meets the needs of the Department of Public Safety and Corrections and our customers. We believe these efforts will be successful and serve as a model that can be used in locations around the country.

Cell detection and managed-access technologies should be considered as superior and preferred alternatives to jamming for two critical reasons: because jamming will not guarantee that contraband wireless devices will be rendered inoperable or that convicts won't be able to communicate with the outside world and because jamming can cause harmful interference to legitimate users. Regarding the first of these points, jamming is not foolproof and, with either a direct line of sight to a cell tower or shielding from the jammer's signal, an inmate in possession of a phone may still be able to complete a call or send a text message.

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

Regarding the second, and more serious of our concerns, for jamming to be effective, correctional administrators will have to jam their entire facilities, fence to fence and everything in between. Absent a commitment to jam the entire facility, the same corrupt individuals who smuggle contraband phones to inmates simply can point out where they can be used outside the range of a jammer. To jam an entire facility and deal with the constantly changing radiofrequency environment, which is impacted by changes in network load, cell tower locations, weather, and even the time of year, and the helical way in which radio waves propagate (which contrasts with the linear nature of prison boundaries), will require "over-jamming" in which the harmful signal extends beyond the facility and into areas where legitimate users may be impacted. We know this because the problem of illicit wireless usage in prisons is not unique to the United States, and in other countries where jammers have been employed to thwart this problem, they have caused significant interference beyond their intended range. The laws of physics are universal, and these same problems will occur here if we proceed with the deployment of jamming equipment, especially in areas where correctional facilities are located in urban and suburban environments or adjacent to transportation corridors. This is often the case, as shown in the screen-shots accompanying testimony.

In addition to disrupting commercial wireless service used by persons outside a correctional facility, a system designed to jam wireless calls emanating from within a correctional facility could also jam important public safety communications. The 800 MHz public safety band is adjacent to the cellular band and the 700 MHz spectrum bands that will soon be brought into use by both commercial and public safety entities are interleaved with one another, thus making it quite conceivable that a system designed to jam commercial service might also jam communications used by fire departments or other public safety agencies that might be called upon to operate near or even at a prison. In contemplating the authorization of jammers, the Congress should consider these possibilities and exercise substantial care to protect both the public and public safety users.

In our view, that care should start with a bias in favor of non-interfering technologies. However, if jamming is to be considered, the proper approach would be to start with rigorous FCC lab and field testing, involving industry engineers, followed by the establishment of rules that would govern the use of certified, tested equipment. Once FCC rules are in place, the Commission could consider case-by-case requests for the use of jammers. In evaluating such requests, the Commission should consider what technical alternatives are available, what actions have been taken to prevent the smuggling of wireless devices into the applicant's facility or facilities, what procedures have been employed to locate and confiscate unauthorized devices, and why those procedures have proven inadequate, as well as the location of the facility for which authorization to jam is being sought. In areas where a facility is in close proximity to commercial or residential properties, or to major transportation corridors, jamming may not be appropriate even under tightly controlled circumstances and the Commission must weigh the public interest in evaluating requests for authorization to jam.

Strong post-deployment safeguards also would be necessary in the event that jamming is authorized. Devices must be subject to strict chain-of-custody requirements and include remote shut-down capabilities to prevent them from falling into the wrong hands and being used inappropriately. Additionally, aggressive post-deployment monitoring should be employed to identify interference.

Even with these safeguards in place, interference is likely, and public safety and wireless carriers will not know about instances of interference until after they occur. This forces the industry and public safety to react, and in an instance where a citizen's or public safety official's safety or well-being is at stake, reacting after the fact may be too late.

While CTIA strongly supports the underlying goal of S. 251, and although the new draft of the legislation does contain several improvements over the introduced version of the bill, we remain troubled that the bill turns the process of testing, setting rules, and considering applications for authorization on its head. The bill would permit applications for authorization to deploy jammers upon enactment and require the FCC to act on any such application within 60 days, yet it does not require testing and the establishment of rules to be completed for one year. This process must be reversed.

Additionally, the bill lacks any reference to alternative, non-interfering technologies. The deployment of technology that includes the possibility, in fact likelihood, of interference will impose on the industry the burden and cost associated with regular field-testing and monitoring near thousands of correctional facilities; a better, less burdensome approach would be to require periodic, but unannounced testing by the FCC. The best approach, however, would be to give preference to non-interfering alternatives so that the problems associated with jamming are avoided altogether and law enforcement's ability to gather intelligence by way of wiretaps is preserved.

Finally, the bill is incomplete because it fails to address the supply and demand problem at the heart of this issue. We urge Congress not to lose sight of why we have this problem or, put differently, how wireless handsets are getting in to correctional facilities.

Fundamentally, as the title of the hearing suggests, this is a contraband issue and the Congress and many states need to update and enforce their contraband statutes to impose tougher penalties for the possession, provision, or support of contraband handsets. Unfortunately, even prison officials acknowledge that "the most common method used by the inmate population for obtaining cell phones is through the use of corrupted staff" at correctional institutions.[3] This conclusion has been repeated by

[3] Affidavit of John R. Campbell, Warden, Val Verde Correctional Facility, Del Rio, Texas, filed August 1, 2007 in Petition of the GEO Group, Inc. for Forbearance from Application of Sections 302, 303 and 333 of the Communications Act of 1934, as amended, and Sections 2.803 and 2.807 of the

others, including the Texas inspector general, who recently told Wired magazine that "there is no question that corrupt officers are involved" in the smuggling of contraband wireless devices[4], and Antonio Gioia, a drug prosecutor with the Maryland State Attorney's Office in Baltimore, who told WJZ-TV that "It's not a big secret. They [phones] are chiefly smuggled in by correctional officers."[5] The motive for this activity is financial, as a recent report of the California Office of the Inspector General found that over one year, one "correctional officer received approximately $150,000 for smuggling approximately 150 phones to inmates."[6] Remarkably, while the officer in question was terminated, he faced no legal repercussions for his actions.

This kind of corruption and other efforts to smuggle contraband to prisoners must be stopped by significantly enhancing the penalties associated with this behavior. These efforts also must extend to those who facilitate the use of contraband handsets by paying for service. While the threat of incarceration may not deter those who already are imprisoned, it may cause those who provide illicit wireless devices or enable their use by inmates to stop for fear of facing meaningful time behind bars.

We have seen the imposition of enhanced penalties work in other areas. Three years ago, this Committee was concerned – as we were – with the problem of pretexting. With our full support, congressional action imposing stiffer penalties, including criminal sanctions, helped to quickly and effectively dry up the market for pretexting. That approach should be tried here too, and while several states, including West Virginia, North Dakota, Arkansas, Texas, Florida, Nevada, and Indiana, have recently updated their contraband statutes to include specific penalties for the possession or provision of unauthorized handsets, many states have yet to do so. CTIA encourages

---

Commission's Rules to Allow State and Local Correctional Authorities to Prevent Use of Commercial Mobile Radio Services at Correctional Facilities

[4] Vince Beiser, "Prisoners Run Gangs, Plan Escapes and Even Order Hits With Smuggled Cellphones," Wired, May 22, 2009, available at http://www.wired.com/politics/law/magazine/17-06/ff_prisonphones?currentPage=all

[5] Mike Hellgren, "Calling the Shots: Cell Phones & Crime Behind Bars," available at http://wjz.com/local/cell.phone.contraband.2.999932.html

other states and the Federal government to enact legislation to make the possession, provision, or support of a contraband wireless device a felony.

Many states also need to implement "airport style" security measures for staff and visitors who enter prison grounds. Remarkably, not all states 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 states 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."[7]

Finally, in considering whether action is necessary to allow some limited use of jamming technology, CTIA also urges the Committee to ensure that the FCC actively and aggressively enforces the existing prohibition on the unauthorized use of jammers. Carriers and others who depend on the ability to use spectrum on an interference-free basis are encountering too many cases where individuals have engaged in unlawful "self-help" to jam wireless signals, often with an impact that reaches far beyond their intended target.

Just this spring, CTIA identified the use of a jammer at Mt. Spokane High School in Mead, Washington, where school administrators had installed an illegal jammer to prevent students from using their phones during school hours. As it happened, the jammer also interfered not only with communications between commercial mobile radio service customers, but also with the county sheriff's cross-band repeater, the key to enabling communications between the county's sheriff, local police, and the local SWAT team. One of our carriers that serves western Kansas and eastern Colorado experienced a similar problem when illegal jamming equipment was deployed by the Agate School District in Colorado. We recognize that the FCC's

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

enforcement team is spread thin, but increased attention to, and action against, those who market or deploy unauthorized jammers and other devices that cause interference is both appropriate and necessary.

Thank you for the opportunity to appear on today's panel. I appreciate the opportunity to share the wireless industry's views on this matter and look forward to working with you to achieve a solution to this matter that works to put an end to the use of contraband phones in prisons and preserves reliable wireless service for law-abiding citizens.