

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

**Commission Seeks Comment on Certain
Wireless Service Interruptions**

)
) GN Docket No. 12-52
)
)

INITIAL COMMENTS OF GLOBAL TEL*LINK CORPORATION

Chérie R. Kiser
Matthew L. Conaty*
Cahill Gordon & Reindel LLP
1990 K Street, N.W., Suite 950
Washington, D.C. 20006
202-862-8900 (telephone)
202-862-8958 (facsimile)
ckiser@cgrdc.com

Dated: April 30, 2012

Its Attorneys

TABLE OF CONTENTS

	<u>Page</u>
I. THE SECURITY AND INTEGRITY OF CORRECTIONAL FACILITIES PROVIDES A SOUND BASIS FOR INTERRUPTING WIRELESS SERVICE	5
A. Contraband Wireless Devices in Correctional Facilities Constitute a Significant Risk to Public Safety.....	5
B. Correctional Facilities Have Identified a Clear Public Interest Need to Interrupt Illicit Wireless Activity.....	10
II. PAST PRACTICES AND PRECEDENTS DEMONSTRATE THE CRITICAL IMPORTANCE AND TECHNOLOGICAL FEASIBILITY OF WIRELESS INTERRUPTION TO ENSURE PUBLIC SAFETY	13
A. Domestic Government Actors Have Promoted and Tested Interruption of Wireless Service for Public Safety Purposes.....	13
B. Foreign Governments Have Considered and Effectuated Interruptions of Wireless Service for Public Safety	16
III. MANAGED ACCESS PROVIDES TARGETED WIRELESS INTERRUPTION IN CORRECTIONAL FACILITIES WHILE MINIMIZING UNDESIRABLE SIDE EFFECTS.....	20
IV. MODERN PRISON DESIGN AND MANAGED ACCESS OPERATION MINIMIZE RISKS TO PUBLIC SAFETY FROM WIRELESS INTERRUPTION.....	22
A. Managed Access Solutions for Correctional Facilities Pose Minimal or No Risk to Access to Emergency Services	23
B. The Use of Wireless Interruption Technology on Correctional Facilities Property Poses Limited Risk Beyond The Property Boundaries.....	24
V. WIRELESS INTERRUPTIONS IN CORRECTIONAL FACILITIES ARE LEGAL UNDER THE COMMUNICATIONS ACT AND CONSTITUTION.....	26
A. Wireless Interruptions by Correctional Facilities Government Actors is Legal under the Communications Act	26
B. Wireless Interruption is Ripe for Forbearance under the Commission’s Statutory Forbearance Mandate.....	28
C. The First Amendment Does Not Prohibit Wireless Interruptions in Prisons.....	32
VI. CORRECTIONAL FACILITIES, AS GOVERNMENT ACTORS, MUST BE AUTHORIZED TO RELY ON WIRELESS INTERRUPTIONS TO ADDRESS UNLAWFUL CELL PHONE USE	37
CONCLUSION.....	41

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

**Commission Seeks Comment on Certain
Wireless Service Interruptions**

)
) GN Docket No. 12-52
)
)

INITIAL COMMENTS OF GLOBAL TEL*LINK CORPORATION

Global Tel*Link Corporation (“GTL”) respectfully makes this submission in response to the request of the Federal Communications Commission (“Commission” or “FCC”) for comments to “inform Commission deliberations regarding whether—and if so, specifically what—legal or policy guidance may be appropriate to provide” in “situations where one or more wireless carriers, or their authorized agents, interrupt their own services in an area for a limited time period at the request of a government actor, or have their services interrupted by a government actor that exercises lawful control over network facilities.”¹

GTL provides secure, customized, highly-specialized telecommunications services to correctional facilities throughout the United States. GTL serves all types of correctional facilities, from nearly 800 county jails to Departments of Correction located in 28 states. In the 20 years that GTL has served the corrections industry, inmate calling has progressed from public payphones to sophisticated software-based security systems that aid peace officers in their attempts to prevent or prosecute illegal activities that may originate within or involve prison populations. In recent years, however, there has been an explosion of wireless devices, stymieing the attempts of law enforcement and correctional officers to regulate inmate

¹ GN Docket No. 12-52, Commission Seeks Comment on Certain Wireless Service Disruptions, Public Notice, 2-3 (rel. Mar. 1, 2012).

communications in a safe and consistent way.

Domestic and foreign governments have concluded that only an interruption in wireless service to these devices can fully address this crisis. The Commission should adopt both short-term and long-term measures to this end, with the ultimate goal of comprehensively restoring safety and security in our nation's correctional facilities.

In the short term, the FCC should expand the scope of its PROTECT Initiative,² the revolutionary "series of practical, meaningful solutions to combat cell phone theft" developed in cooperation with wireless carriers.³ As the Commission rightly recognized, the nexus between violent crime and stolen wireless devices lies in the ability of criminals to profit from them. The proposed database will facilitate carrier deactivation of such devices, dramatically reducing their resale value and increasing public safety. Expanding the use of the database to correctional facilities - where wireless devices are not only an important component of black markets, but a tool for the commission of additional crimes - will yield similar positive results.⁴

The PROTECT Initiative highlights the responsibilities of carriers as entities that must act in the public interest. Commercial Mobile Radio Service ("CMRS") carriers operate not as a matter of right, but by virtue of licenses granted pursuant to specific "terms, conditions, and

² The PROTECT Initiative adopts key provisions of H.R. 4247, the Cell Phone Theft Prevention Act of 2012, through Commission-led partnerships with industry representatives. It can serve a similar role in efficaciously implementing measures to deter illicit wireless transmissions in correctional facilities while a more comprehensive solution is developed if necessary.

³ Prepared Remarks on Stolen Cell Phones Initiative of Federal Communications Commission Chairman Julius Genachowski, Washington D.C., 2 (Apr. 10, 2012) ("PROTECT Comments"), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0410/DOC-313512A1.pdf.

⁴ As the Commission has already designated quarterly meetings with police chiefs as a part of the PROTECT Initiative, reports from correctional facility administrators could easily be solicited on an ongoing basis. A progressive partnership between wireless carriers, providers of telecommunications services to correctional facilities, and correctional facilities administrators would assist the development of prison-specific applications and procedures to enable peace officers "to locate, lock and wipe missing smartphones and tablets." PROTECT Comments at 2

periods” of time.⁵ A “fundamental and pervasive” part of the FCC’s authority to issue such licenses is the “power and obligation” to condition them “on compliance with requirements that the Commission deems consistent with the public interest, convenience, and necessity.”⁶

The PROTECT Initiative demonstrates the FCC’s determination that it is incumbent upon CMRS carriers, as gatekeepers of wireless spectrum, to facilitate the introduction of new technologies and practices deemed by the Commission to benefit the public good.⁷

It is likewise necessary for *all* wireless carriers to permit the introduction of wireless interruption technology into this nation’s correctional facilities to the extent that an expansion of the PROTECT Initiative to correctional facilities proves insufficient. Should the long-term solution to illicit wireless device possession and use in prisons require such technology,⁸ it must be in the form of economical, scalable, and targeted managed access solutions.⁹ Wireless carriers, bound to act in the public interest by the terms of their licenses, must universally facilitate these technologies or practices to comprehensively forestall the completion of illicit

⁵ 47 U.S.C. § 301 (noting that FCC retains authority to regulate “radio communications” and “transmission of energy by radio”).

⁶ *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; et al.*, 26 FCC Rcd 13615, ¶ 117 (2011) (noting that the promotion of safety of life and property fulfills the public interest, convenience, and necessity); *see also, e.g.*, Federal Communications Commission, *The Information Needs of Communities*, 2011 WL 2286864, *347 (June 2011).

⁷ In the negotiations leading up to the PROTECT Initiative, AT&T and T-Mobile noted the difficulty of implementing a reliable wireless device identifier on their Global System for Mobile Communications (“GSM”) networks, which rely on tiny subscriber identity module (“SIM”) cards. *See* Rolfe Winkler, Carriers Band to Fight Cellphone Theft, *The Wall Street Journal*, Apr. 9, 2012, *available at* http://online.wsj.com/article/SB10001424052702303815404577334152199453024.html?mod=googlenews_wsj. Given the importance of establishing a common database for stolen devices (lest thieves simply turn their attentions exclusively to GSM handsets), the FCC has required AT&T and T-Mobile to solve these technological challenges in support of its global approach to combating wireless device theft. *See* PROTECT Comments at 3 (“Under today’s announcement the wireless industry will submit quarterly updates to the FCC on progress on these initiatives. If deadlines aren’t met, the Commission will take action.”)

⁸ *Cf.* H.R. 4247 (noting that mobile electronic devices subject to service interruption do not include prepaid devices).

⁹ As GTL explained in its 2011 Petition for Rulemaking, it has explored alternative solutions to this crisis, including detection and jamming. The benefits of managed access technology, explored further herein, led GTL to deploy the first fully-functioning managed access solution sanctioned by the FCC and the wireless industry. *See* AU PRM11WT, *Petition for Rulemaking of Global Tel*Link Corporation*, 4 (filed July 20, 2011) (“GTL Petition”)

transmissions from prison cells.¹⁰ Industry reticence over focused interruption of portions of the electromagnetic spectrum, or selective opt-out on the part of particular carriers, will have disastrous consequences akin to a partial implementation of the PROTECT Initiative.

Prompt action is needed, as evinced by the testimonies of domestic authorities who are eager to embrace wireless interruption as a tool for ensuring security, as well as the experience of foreign authorities who have actually done so. Technological solutions are urgently required in light of the growing threat to public safety and correctional facilities security posed by inmate use of wireless devices to facilitate escapes and commit crimes, and the inefficacy of existing security measures to deter it. The Commission's consultation with experienced prison administrators, coupled with its leadership in compelling cooperation from CMRS carriers, will ensure that such measures are utilized in a responsible and minimally-intrusive fashion. Managed access systems are a key part of the solution, and the limited risk posed by their use to public safety and non-incarcerated wireless users is far out-weighed by the public interest benefit.¹¹ Close review of pertinent provisions of the Communications Act of 1934, as amended (the "Act"),¹² as well as precedent regarding First Amendment rights in prisons, indicates that wireless interruption can be legally implemented in correctional facilities. "Practical, meaningful solutions" to the problem of wireless devices in prisons are available today. It is incumbent upon the Commission to coordinate the efforts of telecommunications service

¹⁰ Cf. Alyssa Newcomb, FCC, Wireless Carriers Will Create National Database To Fight Smartphone, Tablet Thefts, ABC News, Apr. 10, 2012 ("The burgeoning market for stolen smart phones and tablet devices is the target of a new partnership between the FCC, law enforcement and wireless carriers, who announced today a plan to create a national database that would render the stolen devices worthless. . . . 'If the industry can help dry up the demand, we will take the profit motive away from the criminals,' said Christopher Guttman-McCabe, a vice president at CTIA, a wireless trade group"), <http://abcnews.go.com/Technology/fcc-wireless-companies-create-stolen-smartphone-database/story?id=16107358#.T4wxZ9WDnTo>.

¹¹ See, e.g., CTIA, Contraband Cellphones in Prison (Mar. 2011) (noting CTIA's support for "legal – and proven – technologies such as cell detection and managed access"), http://www.ctia.org/advocacy/policy_topics/topic.cfm/TID/58.

¹² 47 U.S.C. § 151 *et seq.*

providers working to implement these solutions for correctional facilities with CMRS carriers to ensure their cooperation, which is essential to permit these important government actors to exercise control over network facilities to combat this ever increasing public threat.

I. THE SECURITY AND INTEGRITY OF CORRECTIONAL FACILITIES PROVIDES A SOUND BASIS FOR INTERRUPTING WIRELESS SERVICE

A. Contraband Wireless Devices in Correctional Facilities Constitute a Significant Risk to Public Safety

State and federal legislative initiatives have documented the threat to public safety borne by unfettered wireless service in prisons, and the need to establish control by means other than the detection and confiscation of wireless devices. The danger continues to grow with the passage of time, with the “develop[ment] [of] improved means to detect, locate and defeat the use of unauthorized wireless communications devices” now listed as one of the National Institute of Justice’s ten “high-priority research, development and evaluation needs of corrections professionals.”¹³

According to a September 2011 Federal Bureau of Prisons (“BOP”) report, the number of cellular phones confiscated by the BOP from 2008 to 2010 rose from 255 to 1,161 in high, medium, and low security institutions, and from 1,519 to 2,523 in minimum security institutions.¹⁴ The BOP, and representatives from eight state correctional agencies - California, Florida, Maryland, Mississippi, New Jersey, New York, South Carolina, and Texas - named cellular phones “a major security concern,” given their centrality in furthering criminal activity.¹⁵ BOP officials contend that inmates with cellular phones can “circumvent the approved prison

¹³ National Institute of Justice, Corrections Research Priorities (Mar. 12, 2009), <http://www.nij.gov/topics/corrections/priorities.htm>; *see also* PROTECT Comments at 1 (“But the rapid adoption of smartphones and tablets is also creating very real safety concerns. The numbers are alarming.”).

¹⁴ United States Government Accountability Office, Bureau of Prisons: Improve Evaluations and Increased Coordination Could Improve Cell Phone Detection, 20 (Sept. 2011), *available at* <http://asca.net/system/assets/attachments/3456/GAO%20Cell%20Phone%20Report.pdf?1315421670>.

¹⁵ *Id.* at 19.

telephone system and thus are able to hold unmonitored conversations,” enabling them to “arrange the delivery of contraband drugs or other goods, transmit information on prison staff to or from non-inmates, harass witnesses or other individuals, or potentially coordinate an escape.”¹⁶

On February 16, 2012, the Georgia House of Representatives passed H.R. 1325, urging Congress to amend the Act and Commission rules to permit the use of “cellular jammers” in prison facilities.¹⁷ The resolution was predicated on, *inter alia*, the centrality of public safety as an essential function of government, an “epidemic of organized crime and gang related violence” within the nation’s prison system, and the contribution of illegal cellular phone use to attacks on prison staff.¹⁸ The resolution also cited the Georgia Department of Corrections in concluding “that the only cost-effective technology to resolve the problem of illegal cell phone usage in prisons is the use of ‘cellular jammers,’” per confiscation of “8,500 illegal cell phones as contraband” in 2011, and the “hospitalization of 15 inmates, and serious injury to a correctional officer” in cellular phone organized gang fights.¹⁹ As discussed below, however, amendment of the Act is not necessary to effectuate the purpose of the Georgia resolution.

A similar resolution, A.R. 30, was introduced in 2012 by New Jersey Rep. Craig Coughlin.²⁰ The resolution found “that the use of contraband cellular telephones by prisoners in correctional facilities has led to a number of very serious problems,” enabling them “to conduct drug deals, intimidate witnesses, plot violent crimes, and manage criminal enterprises from within these facilities,” which could be halted by, *inter alia*, “requir[ing] the New Jersey

¹⁶ *Id.* at 23.

¹⁷ H.R. 1325, 2012 Reg. Sess. (2012).

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ A.R. 30, 215th Leg., 2012-13 Sess. (2012).

Department of Corrections to block cellular telephone signals within correctional facilities . . .”²¹

In 2009, California correctional facilities implemented Operation Disconnect, an initiative to halt cellular phone smuggling.²² From 2009 through mid-2011, only 432 unauthorized cell phones were seized under the program.²³ Meanwhile, wireless devices continued to proliferate amongst inmates - in 2010, more than 10,000 were either seized from prisoners or found abandoned in cells, common areas, or prison yards.²⁴ In the same year, serial killer Charles Manson was found with an LG flip phone under his prison mattress.²⁵ As then-Governor Arnold Schwarzenegger stated in 2010, the advanced abilities and decreasing size of wireless devices means that “the threat these devices pose to employees in correctional facilities and the public at large has grown. . . . allow[ing] inmates to plan prison assaults and escapes, harass and intimidate witnesses and victims, and facilitate other criminal activities, including directing the activities of criminal street gangs and authorizing murders.”²⁶

The September 2010 “Operation Cellblock” test of managed access technology, performed by GTL, Tecore, Inc. (“Tecore”), and the Mississippi Department of Corrections (“MSDOC”), was prompted in part by the profitability of furnishing illicit wireless devices to inmates. MSDOC visitors and staff receive from \$300 to \$500 to smuggle a cell phone into prison.²⁷ Despite state laws against possession of cellular phones by inmates, MSDOC seized

²¹ *Id.*

²² Michael Montgomery, Program fails to stem flow of cell phones into prison, California Watch, Apr. 22-2011 (“Montgomery Article”), <http://californiawatch.org/dailyreport/program-fails-stem-flow-cell-phones-prisons-9932>.

²³ *Id.*

²⁴ *Id.*

²⁵ Jack Dolan, Charles Manson had a cellphone? California prisons fight inmate cellphone proliferation, Los Angeles Times, Dec. 2, 2010, *available at* <http://articles.latimes.com/2010/dec/02/local/la-me-prison-cellphones-20101203>.

²⁶ Senate Rules Committee, Office of Senate Floor Analyses, Unfinished Business, S.B. 26, 4 (Sept. 8, 2011), *available at* <http://leginfo.legislature.ca.gov/>.

²⁷ Mississippi Department of Corrections, Office of Communications, “Operation Cellblock” Commissioner Epps Shuts Down Illegal Inmate Cell Phone Usage, Press Release, 1 (Sept. 8, 2010) (“Operation Cellblock Press Release”), *available at* http://www.fcc.gov/pshs/docs/speeches/Illegal_Cell_Phone_Press_Conference_Release.pdf.

some 1,994 illegal cellular phones and 1,412 cellular phone accessories during the first half of 2010.²⁸ MSDOC reports also recorded 26 civilian arrests and 46 staff arrests between 2007 and June 2010 for furnishing or attempting to furnish inmates with illegal cell phones.²⁹

Congress has recognized that the control of wireless service and prison safety go hand-in-hand. On October 10, 2010, the Cell Phone Contraband Act of 2010,³⁰ was signed into law,³¹ criminalizing the possession of a CMRS device by an inmate.³² The legislation sought to address the importation of these phones into federal prisons and their concomitant use “to conduct criminal business outside of prison walls, including directing gang hits, controlling drug trafficking operations and even conducting credit card fraud.”³³

Some deemed the Cell Phone Contraband Act as insufficient to meet the challenges of wireless devices in prisons. Rep. Kevin Brady (R-TX) criticized it as “a baby step - but little more,”³⁴ and advocated for the passage of a companion piece - the Safe Prisons Communications Act of 2009.³⁵ The bill, which passed the Senate but died in House committee,³⁶ was intended to “provide another necessary tool in the effort to ensure that the growing problem of cell phones in prison does not turn into an epidemic,” by establishing a framework to permit “state and Federal prisons to petition the Federal Communications Commission and request to operate a wireless jamming device to block inmates from using cell phones to conduct criminal business from

²⁸

Id.

²⁹

Id.

³⁰

S. 1749, 111th Cong. (2010).

³¹

Cell Phone Contraband Act of 2010, Pub. L. No. 111-225,

³²

18 U.S.C. § 1791(d)(1)(F).

³³

155 Cong. Rec. S10112-01 (daily ed. Oct. 5, 2009) (statement of Sen. Feinstein).

³⁴

156 Cong. Rec. H5791 (daily ed. July 20, 2010) (statement of Rep. Brady).

³⁵

S. 251, 111th Cong. (2009).

³⁶

See The Library of Congress Thomas, Bill Summary & Status 111th Congress (2009 - 2010) S.251 All Congressional Actions, <http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:/temp/~bduw9w:@@Xl/home/LegislativeData.php?n=BSS;c=111l>.

inside prison walls.”³⁷ According to Rep. Brady, the Safe Prisons Communications Act was “a more reliable weapon” against wireless use in correctional facilities.³⁸ Citing cases in Texas “where prisoners on death row made threatening calls to victims, prosecutors and their families,”³⁹ he contended that prison officials should be permitted “to use devices that jam the cell signals - making it impossible for the phones to even work.”⁴⁰ In Rep. Brady’s estimation, “[w]e have the technology to do this and do it in a way that doesn't interfere with legitimate use - such as for communities that live nearby.”⁴¹ Maryland Department of Public Safety and Correctional Services Secretary Gary D. Maynard also spoke in favor of the bill by noting numerous crimes that had been perpetuated by illicit inmate cellular phone use, including a successful prison break in Nevada that resulted in three armed home robberies, a kidnapping, and auto theft, and an escape in Kansas where a mobile phone was used to avoid perimeter patrols.⁴²

³⁷ 155 Cong. Rec. S10112-01 (daily ed. Oct. 5, 2009) (statement of Sen. Feinstein).

³⁸ 156 Cong. Rec. H5791 (daily ed. July 20, 2010) (statement of Rep. Brady).

³⁹ See, e.g., Mike Ward, Two years later, smuggled cell phones still a danger, *Austin Statesman*, Oct. 9, 2010 (“Just over two years have passed since Houston state Sen. John Whitmire picked up his phone and found himself talking with a condemned killer on Texas’ death row, which is supposed to be the most secure part of the state’s penal system and where cell phones are illegal. . . . ‘I know your daughters’ names. . . . I know how old they are . . . where they live,’ Whitmire recalls Richard Lee Tabler, facing execution for killing two Killeen men — and who confessed to killing two strippers, as well — telling him in one of several phone calls over a 10-day period in early October 2008. ‘I still remember his words, his voice. It scared the hell out of me — still does.’ But two years later, after a highly publicized crackdown and zero-tolerance policy on prison contraband that grabbed national headlines, Whitmire knows it could happen again.”), *available at* <http://www.statesman.com/news/texas-politics/two-years-later-smuggled-cell-phones-still-a-963526.html?viewAsSinglePage=true>.

⁴⁰ 156 Cong. Rec. H5791 (daily ed. July 20, 2010) (statement of Rep. Brady).

⁴¹ *Id.* The Safe Prisons Communications Act would have compelled the FCC to grant a ten-year renewable waiver to the Director of the Federal Bureau of Prisons “to permit the installation of devices for the sole purpose of preventing, jamming, or interfering with wireless communications within the geographic boundaries of a specified prison, penitentiary, or correctional facility under his or her jurisdiction,” and adopt regulations governing approved devices, such that they “operate the device at the lowest possible transmission power necessary to prevent, jam, or interfere with wireless communications by inmates; and . . . operate . . . in a manner that does not interfere with wireless communications that originate and terminate outside the area of the prison, penitentiary, or correctional facility, by operating the device on a directionalized basis, by utilizing all other interference-limiting capabilities available to the device, or otherwise. Safe Prisons Communications Act of 2009, H.R. 560, 111th Cong. (2009).

⁴² Maryland Department of Public Safety and Correctional Services, Testimony of Gary D. Maynard, Secretary Maryland Department of Public Safety and Correctional Services, S. 251, The Safe Prisons Communications Act of 2009, 2-4 (July 15, 2009), *available at* http://www.asca.net/system/assets/attachments/872/Gary_Maynard_s_S.251_Testimony_7-15-09.pdf?1280164838.

B. Correctional Facilities Have Identified a Clear Public Interest Need to Interrupt Illicit Wireless Activity

As demonstrated in the foregoing sections, nowhere is the need for public safety so acute - nor the consequences of permitting unbridled communications access so great - as in this nation's correctional system. Existing security measures⁴³ are simply inadequate to stem the flow of illicit wireless devices into prisons. Even the most rigorous of security measures can be overcome with "the sometimes-extraordinary resourcefulness of inmates to devise methods to sneak contraband into their cells. . . . transport[ing] cell-phone components into prison via methods as seemingly extreme as ingestion and excretion."⁴⁴ Outside aid also overcomes internal security, "with one popular method of delivery being the insertion of cell-phone components — which are shrinking with each generation of devices — into Nerf balls that can be launched over the walls of corrections facilities."⁴⁵ Once inside, cell phone calls are impervious to the monitoring and recording safeguards attached to payphones, depriving law enforcement officers of vital knowledge concerning inmate communications.⁴⁶

Departments of correction across the country need - and fervently desire - a technological solution to this critical public safety and security issue. In 2009, the Commission was petitioned by 32 state and regional prison systems (led by the South Carolina Department of Corrections ("SCDOC")) to oversee "carefully regulated correction facility jamming" as "part of the package

⁴³ Numerous statutes and regulations across the nation have attempted to address the proliferation of wireless devices in prisons by declaring them to be contraband. *See, e.g.*, 18 U.S.C. § 1791(a), (d)(F); Ark. Code § 5-54-119; Cal. Penal Code §§ 4575(a), 4576; Colo. Rev. Stat. § 18-8-204(1), (2)(n); Del. Code tit. 11, § 1256; Fla. Stat. § 944.47(1)(a)(6); 720 Ill. Comp. Stat. 5/31A-1.1(a), (c)(2)(xi); La. Rev. Stat. § 14:302(E)(7); Mich. Comp. Laws § 800.283a; Okla. Stat. tit. 10A, § 2-7-61(B)(2), tit. 57, § 21(E); Or. Admin. R. 291-016-0100(2); 18 Pa. Cons. Stat. § 5123(c.1), (c.2); Tex. Penal Code § 38.11(a)(3); Va. Code § 18.2-431.1.

⁴⁴ Donny Jackson, Arresting Developments, Urgent Communications, 2, Aug. 1, 2010 ("Jackson Article"), http://urgentcomm.com/policy_and_law/mag/inmate-contraband-cell-phone-201008/index1.html.

⁴⁵ *Id.*

⁴⁶ *See* Federal Communications Commission, *Contraband Cell Phone Use in Prisons Workshop/Webinar*, Transcript, 33 (Sept. 30, 2010) ("Webinar Transcript") (statement of Christopher Epps, Commissioner, Mississippi Department of Corrections), *available at* <http://www.fcc.gov/pshs/docs/summits/contraband-cell-use-transcript.pdf>.

of solutions to protect public safety.”⁴⁷ In a 2009 National Telecommunications Information Administration (“NTIA”) proceeding on contraband cell phone use, Maryland Governor Martin O’Malley and Secretary Maynard requested that ongoing contraband detection be supplemented with technology.⁴⁸ Secretary Maynard subsequently stated on behalf of the Association of State Correctional Administrators (“ASCA”) that correctional officers need to “be equipped with all the tools available to control the illegal activity that cell phones allow,” including “managed access technology and jamming of cell phone signals,” in order to carry out their mission.⁴⁹

New Jersey Corrections Commissioner Gary Lanigan has echoed this conclusion, advocating for technology that would reduce a smuggled cell phone to “a 4-ounce piece of garbage.”⁵⁰ SCDOC Director Jon Ozmint has spoken publicly of the inability of prison officials to cope with the influx of wireless devices - “[a]ll the cell phone detections, all the shakedowns, all the best efforts of our people, and we're pretty good at what we do, we were unable to keep cell phones from coming into our system.”⁵¹ Based on the results of the South Carolina prison

⁴⁷ WT Docket No. 09-30, Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS; et al., Petition for Rulemaking of South Carolina Department of Corrections, 2 (Aug. 6, 2009) (“SCDOC Petition”).

⁴⁸ Letter from Martin O’Malley, Governor of Maryland, and Gary D. Maynard, Secretary, Department of Public Safety and Correctional Services, to Richard K. Orsulak, Emergency Planning and Public Safety Division, Office of Spectrum Management, National Telecommunications and Information Administration (NTIA), 2 (June 11, 2010) (“O’Malley Letter”), available at <http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/Maryland%20Comments%20%20100611.pdf>.

⁴⁹ Webinar Transcript at 13-14 (statement of Gary D. Maynard, Secretary, Maryland Department of Public Safety and Correctional Services, Director, Southern Region, ASCA).

⁵⁰ Star-Ledger Staff, N.J. corrections chief pushes for cell phone jamming technology in prisons, New Jersey Star-Ledger, Aug. 2, 2010, available at http://www.nj.com/news/index.ssf/2010/08/cell_phones_are_hot_commoditie.html.

⁵¹ Webinar Transcript at 34-35 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections). Foreign authorities have reached similar conclusions regarding the dangers of unrestricted wireless service in prison. The chairman of the Independent Monitoring Board of Britain’s largest prison opined that an illicit cell phone trade worth some £9 million annually (a trade that “fuel[s] prison drug trading, bullying and gang problems”) could be curtailed with a £250,000-per-prison investment for jamming systems. BBC News, Nov. 23, 2009, <http://news.bbc.co.uk/2/hi/8373557.stm>. This was particularly poignant in light of inadequate cell phone smuggling laws, in that “three times as many mobile phones were in circulation within prisons as had been seized. . . [with] [e]ver--smaller handsets allow[ing] phones to be smuggled in by prisoners, visitors or corrupt staff. . . [or] thrown over prison walls.” *Id.* Australia’s Corrective Services Administrators’ Council Emerging Technology Working Group has made similar observations on the decreasing size and increasing capabilities of mobile phones -

test, Director Ozmint concluded that managed access works from both technological and cost rationales,⁵² “when you jam those signals, you eliminate that threat. And everybody—the public, law enforcement officers, judges, witnesses—everybody will be safer.”⁵³

In California, a May 2009 Office of the Inspector General Report stated that to truly eradicate cell phone usage, the California Department of Corrections and Rehabilitation (“CDCR”) must coordinate with other correctional agencies to secure the legal and economic basis to employ jamming devices.⁵⁴ Governor Edmund H. Brown Jr. issued an executive order on October 6, 2011, calling for strong measures to ensure public safety and secure operations of California prisons.⁵⁵ One such measure is a “system to intercept and block prisoners’ unauthorized cellular transmissions . . .”⁵⁶ Governor Brown consequently ordered “the CDCR [to] develop and deploy a cost-efficient system to interrupt unauthorized cellular transmissions at California’s prisons in a manner consistent with federal law.”⁵⁷ Despite the legal and regulatory uncertainty surrounding wireless interruption, the State of California has determined that the

ACMA, Australian Corrective Services Administrators’ Council Emerging Technology Working Group, Issues with Mobile Phones in Australian Correctional Centers, 13 (2009) (“ACMA Report”), *available at* http://www.acma.gov.au/webwr/_assets/main/lib311281/csac_submission.pdf - warranting the development and deployment of wireless interruption technology that renders them completely useless within a prison. Australian Communications and Media Authority IFC 02/2010, Review of Mobile Phone Jammer Prohibition, Comments of Corrective Services Administrators’ Council Emerging Technology Working Group, 5 (July 4, 2010).

⁵² SC Prisons try alternative cell phone intercept system, WIS-TV, Oct. 5, 2010, <http://www.wistv.com/story/13244837/fcc-discussing-cell-phone-jamming-in-prisons?clienttype=printable>.

⁵³ Ozmint speaks out on prison contraband cell phone use, South Carolina Radio Network, Oct. 1, 2010, <http://www.southcarolinaradionetwork.com/2010/10/01/ozmint-speaks-out-on-prison-contraband-cell-phone-use/>; *cf.* Webinar Transcript at 35 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections) (“And so what cell phones enabled folks on the inside to do was to create a new pipeline for contraband. And the new pipeline for contraband in our state is simply throwing, shooting, dropping, flying, packages full of cell phones over the fence line. And because they’re able to communicate with the person on the inside, the folks on the outside know exactly when and where to throw. And if we intercept, and we have good intelligence right now that indicate we’re getting about 75 percent of the phones coming in.”).

⁵⁴ State of California Office of the Inspector General, Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety, 2 (May 2009), *available at* http://www.asca.net/system/assets/attachments/866/California_OIG_Report_on_Inmate_Cell_Phone_Use.pdf?1280164472.

⁵⁵ Executive Order B-11-11 (Oct. 6, 2011), *available at* <http://gov.ca.gov/news.php?id=17258>.

⁵⁶ *Id.*

⁵⁷ *Id.*

need for a managed access system for its correctional facilities cannot wait any longer and solicited bids for a system on July 7, 2011.⁵⁸

II. PAST PRACTICES AND PRECEDENTS DEMONSTRATE THE CRITICAL IMPORTANCE AND TECHNOLOGICAL FEASIBILITY OF WIRELESS INTERRUPTION TO ENSURE PUBLIC SAFETY

A. Domestic Government Actors Have Promoted and Tested Interruption of Wireless Service for Public Safety Purposes

The centrality of wireless devices to terrorist plots and crimes committed within correctional facilities has fostered a growing willingness to explore the advantages of such interruptions. Citing then-recent railway bombings in Spain and an attempted assassination attempt against Pakistani President Pervez Musharraf, Los Angeles County Sheriff Lee Baca proposed a cell phone jamming plan in May 2004 to take effect upon warning of a terrorist attack. A Los Angeles *Daily News* article questioned the feasibility of such a plan under existing law, as well as potential effects upon first responders from an overly-broad frequency blackout. Still, it cited the ongoing use of jammers in specific high-risk situations, such as by hospital officials to prevent interference with heart defibrillators, the Secret Service to protect the president when he travels or gives a speech, or law enforcement officials during hostage

⁵⁸ California Technology Agency IFB 11-127805, Inmate Ward Telephone System and Managed Access System Services, Invitation for Bids (July 7, 2011) (“California IFB”), *available at* <http://www.bidsync.com/DPX?ac=view&auc=1810550>; *see also, e.g.*, Jeff Webster, California CDCR seeks proposals for contraband cell phone managed access, GovWin, July 13, 2011 (“Earlier this month, the California Department of Corrections and Rehabilitation (CDCR) began the process of replacing its current contract for inmate telephone services through competitive procurement . . . The state concluded that a managed access system was the only currently-available technology to allow signal access to certain devices while prohibiting access to other devices. Given current federal law, the jamming of communications is illegal, and the cost of using signal triangulation would be too high. The decision to use a managed access system is estimated to cost between \$18 million and \$35 million. The system will draw unauthorized cell phone signals to an onsite, mock, high-signal commercial-grade cellular tower that thwarts communications. Authorized cell phone signals are not allowed to connect to this tower and will find a real commercial signal to complete the call. This system will be used throughout 33 adult institutions”), *available at* <http://www.input.com/index.cfm?fractal=blogTool.dsp.blog&blogname=public&alias=California-CDCR-seeks-proposals-for-contraband-cell-phone-managed-access>. GTL has worked closely with the California Department of General Services, Procurement Division, in addressing legal, technological, and economic concerns pursuant to the Invitation for Bids.

situations.⁵⁹ Jamming technology was, for example, used during President Obama's inauguration parade to prevent the detonation of potential remote-controlled bombs, and has been employed during State of the Union addresses and visits by foreign leaders to Washington.⁶⁰

Following several transit bombings in London in 2005, the Department of Homeland Security reached an agreement with CMRS providers under the National Communications System to implement network shutdowns in times of crisis.⁶¹ In 2007, the FBI implemented a pilot program that “deputized about 10 local bomb squads across the country . . . so they could use a small number of radio jammers similar to the military equipment used overseas.”⁶² In 2009, New York Police Commissioner Raymond W. Kelly appeared before the Senate Committee on Homeland Security & Governmental Affairs to testify on “lessons learned” from the November 2008 Mumbai, India terrorist attack.⁶³ Commissioner Kelly noted the ability of “terrorist handlers” to direct operations from outside the engagement zone using portable communication devices.⁶⁴ Consequently, “[w]hen lives are at stake, law enforcement needs to find ways to disrupt cell phones and other communications in a pin-pointed way against terrorists

⁵⁹ Troy Anderson, Cell Phone Block Eyed Baca Exploring Anti-Terror Plan, Los Angeles Daily News, May 9, 2004, *available at* <http://www.thefreelibrary.com/CELL+PHONE+BLOCK+EYED+BACA+EXPLORING+ANTI-TERROR+PLAN.-a0116428926>.

⁶⁰ Spencer S. Hsu, Local Police Want Right to Jam Wireless Signals, The Washington Post, Feb. 1, 2009 (“Hsu Article”), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/01/31/AR2009013101548_pf.html.

⁶¹ EmergiTech, Wireless Signal Jamming: Implications for Jail Management and Policing, <http://www.emergitech.com/company.aspx?id=122>.

⁶² Hsu Article.

⁶³ *Lessons from the Mumbai Terrorist Attacks*, Testimony of Raymond W. Kelly, Police Commissioner, New York Police Department, 111th Cong. (Jan. 8, 2009) (“Kelly Testimony”), *available at* http://www.nyc.gov/html/nypd/html/pr/lessons_from_mumbai_terror_attacks.shtml.

⁶⁴ *Id.*; *see, e.g.*, Somini Sengupta, Dossier Gives Details of Mumbai Attacks, N.Y. Times, Jan. 6, 2009 (describing an Indian dossier detailing “previously undisclosed transcripts of telephone conversations, intercepted by Indian authorities, that the 10 gunmen had during their killing spree”), *available at* <http://www.nytimes.com/2009/01/07/world/asia/07india.html?fta=y>.

using them.”⁶⁵

The Commission entered into a partnership in 2009 with state corrections departments and agencies “such as the National Institute of Justice, the Federal Bureau of Prisons, and the National Telecommunications Information Administration, national organizations including the American Correctional Association and Association of State Correctional Administrators, as well as vendors and wireless carriers, to explore the most effective and precise technological options to defeat contraband cell phone use.”⁶⁶ In February 2010, the NTIA, acting at the direction of Congress,⁶⁷ conducted two tests of wireless detection and control systems at the Institute for Telecommunications Sciences in Boulder, Colorado and the Federal Bureau of Prisons Minimum Security Facility in Cumberland, Maryland.⁶⁸ Emissions were produced in cellular, PCS, GPS, and public safety bands, but as a whole, prison operations were unaffected.⁶⁹ Reflecting on the Maryland NTIA tests, Governor O’Malley and Secretary Maynard noted that “the jamming technology worked within the prison and there was no interference with federal operations within the testing area. . . . [the] test demonstrated that jamming can work without interfering with or compromising public safety.”⁷⁰

⁶⁵ Kelly Testimony.

⁶⁶ Jamie Barnett, Chief, FCC Public Safety & Homeland Security Bureau, Operation Cellblock: A New System to Combat Use of Contraband Cell Phones in Prisons, Prepared Remarks, 1 (Sept. 8, 2010), *available at* http://www.fcc.gov/pshs/docs/speeches/Parchman_Contraband_Cell_Remarks.pdf.

⁶⁷ U.S. Department of Commerce, *Contraband Cell Phones in Prison: Possible Wireless Technology Solutions*, 1 (Dec. 2010) (“NTIA Report”), *available at* http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf; see also H.R. Rep. No. 111–366, at 619 (2009); see NTIA Docket No. 100504212-0212-01, *Preventing Contraband Cell Phone Use in Prisons*, Notice of Inquiry (rel. May 12, 2010) (“NTIA NOI”).

⁶⁸ Federal Communications Commission, Public Safety and Homeland Security Bureau, Association of State Correctional Administrators Summer Meetings - 2010, Special Symposium on the Illegal Use of Cell Phones in Prisons, 3 (July 30, 2010) (“FCC Special Symposium”), *available at* http://www.asca.net/system/assets/attachments/986/FCC_Barnett_ASCA_Special_Symposium_DFT_072610.pdf?1282310719.

⁶⁹ NTIA Report at 8.

⁷⁰ O’Malley Letter at 2.

In September 2010, SCDOC Director Ozmint launched a pilot program to test the feasibility and effect of managed access systems.⁷¹ In the same month, GTL, Tecore, and the MSDOC commenced “Operation Cell Block,” a test of managed access technology to intercept cell phone transmissions within a designated area, while still permitting emergency calls.⁷² Some 216,320 contraband wireless call attempts were captured and prevented from connecting in the first month of the program,⁷³ prompting MSDOC Commissioner Christopher Epps to hail managed access as a “solution” to the problem of cellular phones in prison.⁷⁴ The tested managed access system addressed not only inmate calling, but also postage stamp-sized SIM cards, which store contact lists and account plans and facilitate communication by being traded between phones.⁷⁵ In February 2012, the CDCR reported that its own 2011 test of managed access systems over an 11-day period “detected a total of 2,593 unique wireless devices and blocked more than 25,000 unauthorized communication attempts (calls, texts, emails, efforts to log on to the Internet from a smart phone, etc.), or an average of 2,500 per day.”⁷⁶

B. Foreign Governments Have Considered and Effectuated Interruptions of Wireless Service for Public Safety

Wireless interruption technology has also been enthusiastically adopted by foreign

⁷¹ Meg Kinnard, SC prisons chief says he's testing technology to block calls of inmates' smuggled cell phones, Minneapolis-St. Paul Star Tribune, Oct. 1, 2010, *available at* http://www.startribune.com/templates/Print_This_Story?sid=104144568.

⁷² Operation Cellblock Press Release at 1.

⁷³ Webinar Transcript at 5, 31 (statement of Christopher Epps, Commissioner, Mississippi Department of Corrections).

⁷⁴ *Id.* at 31-32 (statement of Christopher Epps, Commissioner, Mississippi Department of Corrections). Commissioner Epps also explained that he “put in the policy here in Mississippi that effective October 1st [2010] and thereafter any inmate caught with a cell phone in the State of Mississippi will be transferred to Parchman”

⁷⁵ Global Tel*Link, Mississippi DOC Launches First Managed Access System In The U.S. by Deploying Tecore’s iNAC™ To Fight Contraband Cell Phones in “Operation Cellblock,” iNAC Prevents Unauthorized Communications, Permits Authorized and 911 Calls, and Complies with Communications Act with Support of Commercial Carriers, Press Release (Sept. 2010) (“GTL Press Release”), *available at* http://www.gtl.net/about/GTL_and_Tecore_Networks_Press_Release.shtml.

⁷⁶ California Department of Corrections and Rehabilitation, Fact Sheet, 2 (Feb. 2012), *available at* <http://www.cdcr.ca.gov/Contraband-Cell-Phones/docs/Contraband-Cell-Phone-Fact-Sheet-January-2012.pdf>. The CDCR noted that its representatives, as well as those of the California Technology Agency, had visited the Mississippi and South Carolina tests

governments to monitor and control correctional facility communications.⁷⁷ The 1999 European Community (“EC”) Directive explicitly exempts radio equipment and telecommunications terminal equipment from certification in matters involving “the activities of the State in the area of criminal law.”⁷⁸ Swedish law prescribes fines or incarceration for “transmitters used to jam mobile telephony,” as such devices can cause substantial damage “to communication systems that are necessary to society, such as mobile telephony or the emergency services radio communications.”⁷⁹ Nonetheless, the Swedish Post and Telecom Authority is empowered to “provide for an exception to the prohibition on possession of jammers on behalf of the Prison and Probation Administration, for jammers to be used in prisons.”⁸⁰

Germany has implemented signal jamming systems on a cell-by-cell basis in prisons throughout the country.⁸¹ Baden-Württemberg led the movement in 2008, installing small-range signal jammers after state authorities found 153 contraband cellular phones amongst prisoners in 2007.⁸² Baden-Württemberg Minister of Justice Ulrich Goll concluded that the rollout was a “complete success,” as the devices increased internal security without interfering with signals made outside prison walls.⁸³

The Australian Communications and Media Authority (“ACMA”) opened a docket in 2010 seeking comment on the possibility of moderating or eliminating a long-standing prohibition on mobile phone jamming. ACMA sought particular input on the potential for an

⁷⁷ Cf. PROTECT Comments (“Finally, the database system will become more effective as more countries join. We have called on all countries to adopt the database and other solutions we’re announcing today, and I am making it a priority of the FCC’s International Bureau to work with other countries to advance this initiative.”).

⁷⁸ Council Directive 99/5, 1999 O.J. (L019) 10-28 (EC) at art. 1 (“EC Directive”).

⁷⁹ PTS, Förbud mot störsändare, <http://www.pts.se/sv/Radio/Utrustning/Forbud-mot-storsandare/>, (“Förbud mot störsändare”), *translated*, translate.google.com.

⁸⁰ *Id.*

⁸¹ Elmir Majstorić, Mobile phones in prisons are a big security flaw, a&sAdria, Oct. 20, 2010 (“Majstorić Article”), *available at* <http://www.asadria.com/articles/2/0/2.html>.

⁸² *Id.*

⁸³ *Id.*

exemption to the ban to facilitate the trial of mobile phone jammers at the maximum-security Lithgow Correctional Centre in New South Wales.⁸⁴ The docket itself proceeded from a 2009 submission by the Corrective Services Administrators' Council Emerging Technology Working Group,⁸⁵ which advocated for “[c]o-operation and flexibility between correctional services providers, relevant government departments and telecommunications carriers . . . to explore the various mobile phone jamming technologies and address safety concerns associated with any new technologies being introduced into prison facilities.”⁸⁶

In New Zealand, government officials and wireless carriers have forged a partnership to ensure the long-term security of correctional facilities. In August 2007, the Department of Corrections and the country's two largest carriers, Vodafone and Telecom New Zealand, signed a Memorandum of Understanding (“MOU”).⁸⁷ The MOU provided for the implementation of “mobile phone blocking” systems, intended to prevent inmates from committing additional crimes while incarcerated.⁸⁸ The MOU also laid the groundwork for a telecommunications industry code - the 2009 Code for the Control of Unauthorised Use of Mobile Phones in Prisons -

⁸⁴ Australian Communications and Media Authority, Review of the Mobile Phone Jammer Prohibition, 1 (Jan. 2010), *available at* http://www.acma.gov.au/webwr/_assets/main/lib311281/review_of_mobile_phone_jammer_prohibition.pdf.

⁸⁵ *Id.*

⁸⁶ ACMA Report at 13; *see also, e.g.*, Jo Best, Stop jail mobile jammer delays now: Minister, ZDNet Australia, June 25, 2007 (“NSW Justice Minister John Hatzistergos has demanded the federal government be quicker to embrace phone jamming in jails. Hatzistergos said phone jammers must be introduced into state correctional facilities as a matter of urgency, adding in a statement the use of mobiles by prison inmates “poses a serious threat to the security, good order and discipline of our correctional centres.”), <http://www.zdnet.com.au/stop-jail-mobile-jammer-delays-now-minister-339279038.htm>.

⁸⁷ Elena Balan, *Prisons Will Jam All Mobile Phone Use*, Softpedia, Aug. 22, 2007, <http://news.softpedia.com/news/Prisons-Will-Jam-All-Mobile-Phone-Use-63389.shtml>.

⁸⁸ Vodafone, Corporate Responsibility, Mobile phone blocking in prison (“Vodafone Corporate Responsibility”), <http://www.vodafone.co.nz/about/corporate-responsibility/social-impact.jsp>; *see also, e.g.*, Australian Mobile Telecommunications Association, Mobile phone jamming introduced to New Zealand prisons, (“New Zealand Corrections Minister Phil Goff explains that “[t]he blocking technology complements the monitoring system on prison pay phones across the country. All prisoner phone calls at prisons are recorded and monitored by Corrections intelligence teams on both a targeted and random basis. Since the telephone monitoring was piloted in November, evidence gathered has led to charges against prisoners around the country for robberies, harassment, gang activity, illegal drug use and a raft of other offending.”), <http://www.amta.org.au/articles/amta/Mobile.phone.jamming.introduced.to.New.Zealand.prisons>.

that requires wireless carriers to “grant Spectrum Licences to the Department of Corrections to allow the Department of Corrections to detect, monitor, disrupt, interfere and disable wireless transmissions relating to mobile phones and/or electronic radio communication Devices.”⁸⁹ In return, the Department of Corrections must provide wireless carriers with detailed technical specifications of transmitting equipment and prison facilities.⁹⁰

New Zealand’s wireless carriers and the Department of Corrections had begun working together in 2005, in the shadow of “concerns that the [blocking] equipment could affect users outside prison walls.”⁹¹ As a result, the parties had tested a variety of technologies, including “detectors which identify mobile telephone activity within an area; local blanket jammers which block mobile telephone signals in a localised area; micro cell jammers (towers) which block mobile telephone use in parts, or all, of a prison site; and hand-held mobile telephone detectors.”⁹² These were evaluated according to the “individual characteristics of each prison . . . in order to determine the suitability of each of the above solutions with reference to the geographical location of the prison, the surrounding area, the proximity of residential and other nearby populated areas and the effect upon legitimate mobile phone users.”⁹³ The tests were successful, and the technology was fully implemented across New Zealand’s 20 prisons by February 2009 at a cost of \$5 million.⁹⁴ According to the Australian Corrective Services Administrators’ Council Emerging Technology Working Group, “New Zealand has . . . advised

⁸⁹ See Telecommunications Carriers’ Forum, Code for the Control of Unauthorised Use of Mobile Phones in Prisons, 5 (Nov. 7, 2008), available at <http://www.tcf.org.nz/library/e7b0100d-e056-4ef7-9d12-c18e5b4fb103.cmr>.

⁹⁰ *Id.*

⁹¹ Jo Best, *Vodafone, Telecom tackle mobile jamming for jails*, ZDNet Australia, Aug. 23, 2007, <http://www.zdnet.com.au/vodafone-telecom-tackle-mobile-jamming-for-jails-339281448.htm>.

⁹² ACMA Report at 12.

⁹³ *Id.* For example, Rimutaka Prison and the Northland Region Corrections Facility, far from any residential center, were deemed ideal locales for mobile telephone blocking towers, “whereas Mt Eden Prison in central Auckland was considered more suited to a combination of local blanket jammers and detectors.”

⁹⁴ Vodafone, Corporate Responsibility; ACMA Report at 13.

that jamming technology can be sited to operate solely within the prison boundaries and that fears about the possible interference with licensed radiocommunications; possible disruption of telecommunications; safety of life issues (such as the interference of 000 calls); interference to licensed services and other services in adjacent spectrum bands; the effect upon legitimate users within a certain radius; and possible radiation levels of jamming devices, particularly in confined areas have not eventuated.”⁹⁵

III. MANAGED ACCESS PROVIDES TARGETED WIRELESS INTERRUPTION IN CORRECTIONAL FACILITIES WHILE MINIMIZING UNDESIRABLE SIDE EFFECTS

Managed access meets the outstanding needs of correctional facilities to combat inmate wireless calling in a minimally invasive fashion. Managed access systems allow particular users (those on a preapproved “white-list”) to make calls from inside a prison, but prohibit the transmission of all other communication.⁹⁶ They operate by detouring the signal emanating from a wireless device to the managed access system's base station. There, the signal is either recognized as “authorized” to transmit and therefore connected to the CMRS carrier's network, or terminated because the signal is not authorized. Operation is predicated on spectrum-leasing arrangements with CMRS providers, as the managed access system must “broadcast” on all of the frequencies being accessed by the wireless devices within the prison borders under surveillance.⁹⁷ Consequently, managed access does not rely on the emission of an active

⁹⁵ ACMA Report at 13.

⁹⁶ Jackson Article at 2; *cf.* Webinar Transcript at 37 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections) (“And it is incredibly precise. I’ve been amazed at how precise that management access antenna, that power level how precise they can be. I was equally amazed with how precise the jamming technology that we saw demonstrated was.”).

⁹⁷ *See, e.g.*, PCS Broadband Special Temporary Authorization File No. 0004345520, Tecore Government Services LLC, Certification (Aug. 5, 2010) (“The service provided on the spectrum leased to TGS (the “Tecore Manages Access™”) does nothing more than manage the access of wireless devices to the existing commercial networks of licensed CMRS operators (the “Macro Networks”) in a defined geographic area within a prison or other correctional facility, in coordinated usage of the licensed spectrum in a radio underlay of the Macro Networks. Tecore Managed Access™ operates within the ‘call set-up’ layer of wireless infrastructure to authenticate permitted

jamming signal, which may engender deleterious side effects in accomplishing its aims.⁹⁸

Managed access systems provide a backstop to prison phone searches, which have proven less and less effective with the passage of time. Correctional officers are assured that any wireless device an inmate manages to obtain will not be able to function, lessening the consequences of an unsuccessful investigation for contraband or a partially-effective jamming system.⁹⁹ This is especially true of SIM cards, which are easy to conceal and can sustain a series of communications in their passage from prisoner to prisoner. In addition, managed access permits correctional facilities to engage in forensic analysis of the device and call information, a vital tool in law enforcement unavailable with conventional jamming.

As the SCDOC and its 38 fellow state and local signatories observed in their 2009 Petition for Rulemaking, “[t]here is no single solution that will solve this problem in the wide variety of state and local correction facilities in our country.”¹⁰⁰ Managed access systems are amongst the most promising, given their innate scalability and adaptability. Through cooperation with CMRS providers, managed access providers can adapt to shifts in spectrum allocation and technological advancement.¹⁰¹ They can be tailored in placement and functionality according to the specific needs and architectural demands of individual correctional

devices for completion of their “calls” (voice, text, or data) by the Macro Networks, while capturing and holding unauthorized device at authentication and disallowing completion of their calls through the Macro Networks.”).

⁹⁸ NTIA Report at 2; *cf.* Webinar Transcript at 83 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections) (“And yes, managed access is interference with a signal. It does stop the signal eventually, but it's not jamming.”).

⁹⁹ *See, e.g.*, The Nation, Search of Khao Bin Prison turns up more illegal objects, Feb. 11, 2012 (“In an impromptu raid on cells in Ratchaburi’s Khao Bin Prison yesterday, officials found many prohibited items including a mobile phone hidden inside a wall, which is a blind spot for the prison’s signal-jamming device. . . . Officials also found a Nokia phone embedded in a wall on the third floor. The phone, which had a SIM card, could be used because that particular area is a blind spot for the signal-jamming device. Officials plan to look for other blind spots within the premises and check on all outgoing numbers to see who called out and for what purpose”), <http://www.thaiprisonlife.com/news/search-of-khao-bin-prison-turns-up-more-illegal-objects/>.

¹⁰⁰ SCDOC Petition at 2.

¹⁰¹ *See, e.g.*, NTIA NOI at 20 (“Any solution to the contraband cell phone problem in prisons needs to address the growing number of telecommunications methods. This includes, for example, the Cellular, PCS, AWS, SMR, WiMAX, 700 MHz and General Mobile Radio bands. Additional methods of telecommunication include satellite, Wi-Fi, and Bluetooth mobile devices.”).

facilities. As evinced by the New Zealand example discussed above, partnerships between government and private stakeholders afford an excellent chance of fully deterring inmate usage of wireless devices with minimal consequences to non-incarcerated third parties.¹⁰²

IV. MODERN PRISON DESIGN AND MANAGED ACCESS OPERATION MINIMIZE RISKS TO PUBLIC SAFETY FROM WIRELESS INTERRUPTION

In 2010, the Commission's Public Safety and Homeland Security Bureau convened a Special Symposium on the Illegal Use of Cell Phones in Prison. In assessing the various technological choices for combating illicit wireless use in correctional facilities, the summary of the symposium identified several key "interdependent issues," including legal and interference concerns, avoiding unintended and harmful consequences, and preserving legitimate consumer, public safety, and 911 wireless communications.¹⁰³

A managed access system inherently fulfills the symposium concerns. Wireless industry representatives who have expressed dismay at the potential side effects of jamming have praised managed access as a "promising technological solution," because of its utilization of "location-determination technologies to ensure that the controls apply only in the geographic area of the prison," and its elimination of interference to legitimate users.¹⁰⁴ A June 2010 study by VComm concluded that a managed access system allows calls placed in prisons to be monitored and

¹⁰² See, e.g., NTIA Report at 25 ("Managed access requires structured coordination and cooperation between a managed access system vendor and the wireless service providers in the affected area. The partnership with the wireless carriers is critical to ensuring the long-term efficacy of the solution as new products and different frequencies are utilized in the wireless landscape.").

¹⁰³ FCC Special Symposium at 5; compare, e.g., Australian Communications and Media Authority IFC 02/2010, Review of Mobile Phone Jammer Prohibition, Comments of Attorney-General's Department, 1 (2010) ("The Federal Offenders Unit of the Department believes that there is a strong operational case for the deployment of mobile phone jammers in correctional centres, subject to technical and legal issues being resolved. However, FOU considers that such deployment should not adversely impact on: (i) the health and safety of inmates, prison staff or people in area surrounding the prison; (ii) the ability of residents and business in the area surrounding the prison to use, and receive calls from, mobile phones, or (iii) emergency services frequencies."), available at http://www.acma.gov.au/webwr/_assets/main/lib311281/attorney_generals_dept_ifc02-2010.pdf.

¹⁰⁴ Contraband Cell Phones in Correctional Facilities: Public Safety Impact and the Potential Implications of Jamming Technologies: Hearing on S. 251 Before the S. Comm. on Commerce, Science & Technology, 111th Cong. 3-4 (2009) (prepared statement of Steve Largent, President & CEO, CTIA-The Wireless Association), available at http://files.ctia.org/pdf/Testimony_CTIA_Largent_Contraband_Cell_Phones_7_15_09.pdf.

directed appropriately, while offering important public safety advantages: it allows E911 emergency calls and CALEA calls within and without prison facilities, transmits at lower levels than jamming systems to effectuate call capture, and “[c]an intercept Nextel/SMR calls within prisons without interfering with Public Safety radios.”¹⁰⁵ Rear Admiral (Ret.) James Barnett, Chief of the FCC’s Public Safety and Homeland Security Bureau, stated that the Commission’s focus has been “on the technologies that are not only lawful, but also specifically target the problem at hand without jeopardizing essential public safety, federal and state law enforcement activities.”¹⁰⁶ Admiral Barnett opined that the technology employed at the September 2010 FCC / GTL Operation Cellblock test might “really . . . be the answer to beating cell phones in prisons” as it renders contraband wireless devices “useless to whoever’s trying to use it. And it still put through 911 calls, and it doesn’t interfere.”¹⁰⁷ According to Admiral Barnett, “[t]he use of managed access technology is an effective way to stop the use of contraband cell phones in prisons. . . . [as it] can be used right now and it does not interfere with vital police and firefighter communications or interrupt 9-1-1 emergency calls from being answered.”¹⁰⁸

A. Managed Access Solutions for Correctional Facilities Pose Minimal or No Risk to Access to Emergency Services

Risks associated with 911 calls are effectively minimized by the fact that emergency services in prison - not just emergency calling - are controlled, designed and implemented by

¹⁰⁵ Mike Katra and Sean Haynberg, VComm Telecommunications Engineering, NTIA Prison Jammer Study, 14 (June 11, 2010), *available at* <http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/VZW%20jamming%20NOI%20comments%206-11-10.pdf>; *see also, e.g.*, NTIA Report at 2 (“However, such systems do permit 9-1-1 and known authorized calls.”), 25 (“A managed access system can provide the desirable result – preventing prisoners from communicating by cell phone with people outside of the prison. However, the system permits authorized users to pass through to the network and all 9-1-1 calls are forwarded as well.”).

¹⁰⁶ Webinar Transcript at 10 (statement of James Arden Barnett, Jr., Chief, Public Safety and Homeland Security Bureau, FCC).

¹⁰⁷ Donny Jackson, Mississippi Showcases Deployment to Halt Prison Cell-Phone Use, Urgent Communications, Sept. 8, 2010, http://urgentcomm.com/networks_and_systems/news/miss-deploys-cell-jammer-20100908/.

¹⁰⁸ Operation Cellblock Press Release at 2.

correctional officials.¹⁰⁹ Emergency service procedures are “deemed to lie fully within [correctional facilities] expertise and discretion and, accordingly, [are] insulated from subsequent judicial review.”¹¹⁰ Correctional officials determine what those procedures will be and how access to the facilities will be managed. They coordinate their efforts directly with public safety answering points (“PSAPs”) and address all unrest or medical concerns arising within the facility directly.¹¹¹ To the extent that emergency calls are even permitted under these systems they rely upon existing prison infrastructure (such as wireline phones), wireless interruption will have no impact. In most cases, inmates have no right to place any calls over cellular telephones (or even possess the telephones themselves), rendering a block on emergency calling a moot point. In South Carolina, for example, state law prohibits the use of any cellular phone on prison property by any individual. Consequently, as SCDOC Director Ozmint observed, “[t]here are no legal 911 calls. . . . There are no legal emergency calls because it is against the law.”¹¹²

B. The Use of Wireless Interruption Technology on Correctional Facilities Property Poses Limited Risk Beyond The Property Boundaries

These consequential issues are attenuated by the rural nature of many correctional facilities. Prior to 1980, only 36% of prisons were located in rural communities and small towns. In the years since, prison construction has occurred primarily in non-metropolitan areas, with some 350 rural counties acquiring new residential facilities.¹¹³ From 1980 to 1991, “new non-

¹⁰⁹ See, e.g., 15 Cal. Code. Reg. § 1200 (designating “facility administrator” as responsible for ensuring the provision of emergency and basic health care to inmates, pursuant to facility security regulations).

¹¹⁰ *Labatt v. Twomey*, 513 F.2d 641, 647 (7th Cir.1975).

¹¹¹ See, e.g., State of Texas Regional ITS Architecture, Interface: Correctional Facilities Operations To County Public Safety Dispatch and PSAP (May 27, 2005), <http://www.consysfec.com/texas/web/yoakum/e/i/189-60.htm>.

¹¹² Webinar Transcript at 16 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections). As Director Ozmint explained of the closed nature of prison societies, “We have plenty of mechanisms for our officers and our staff to be in contact in cases of emergency. We have a variety of methods and every prison system has those methods.” *Id.* at 38.

¹¹³ Tracy Huling, *Building a Prison Economy in Rural America*, in *Invisible Punishment: The Collateral Consequences of Mass Imprisonment* (Marc Mauer & Meda Chesney-Lind, Eds., 2002), available at <http://www.prisonpolicy.org/scans/building.html>.

metro prisons had well over twice the proportion of inmates that might have been expected on the basis of the size of the nonmetro population, and the propensity to locate prisons in rural and small town areas was distinctly greater than it had been in the past.”¹¹⁴ From 1992 to 1994, “new nonmetro prisons amounted to 60 percent of the total” number of prisons built, even though nonmetro areas now have only 20 percent of the U.S. population under 1993 definitions of metro and nonmetro boundaries.”¹¹⁵ The location of many prisons in remote areas lessens the risks inherent in wireless interruption, attenuating the effect of signal management or disruption over a larger area with few non-incarcerated residents. As SCDOC Director Ozmint explained, 80 percent of his maximum and minimum prisons are in the middle of 180, 200 acres of property.¹¹⁶ Thus, “with regard to calls off of prison property, our set back lines in 80 percent of our prisons are such that we're not going to interfere with any legal signals off of prison property.”¹¹⁷ The growing sophistication of CMRS technology also reduces the risk of interference with legal signals off prison property for prisons located in metro areas. As SCDOC has noted, “the explosive growth of the CMRS industry in the past quarter century has resulted from large scale frequency reuse and co-channel and adjacent channel use of the same spectrum by multiple carriers in the same area and adjacent areas,” with ever-decreasing “unintended consequences.”¹¹⁸

¹¹⁴ Calvin L. Beale, *Rural Prisons: An Update*, Rural Development Perspectives, Vol. 11, no. 2, at 25 (1996).

¹¹⁵ *Id.*

¹¹⁶ Webinar Transcript at 16 (statement of Dir. Jon Ozmint, Director, South Carolina Department of Corrections).

¹¹⁷ *Id.* This is also true in the context of prison geography itself, which frequently establishes a security area for prisons demarcated by a large spatial buffer. Given that the public does not have access to this area - and the residents within it are prohibited from possessing and using wireless devices - any secondary interference with wireless operations would be of limited concern.

¹¹⁸ SCDOC Petition at 10 (“Such unintended consequences of present frequency reuse have not materialized because it is done well with careful planning. Rather than causing interference, it enables the great benefits of increasing spectrum utilization. Similarly, careful planning of CMRS jamming in corrections facilities where it is possible will result in the intended jamming within the facilities and no harmful interference to other legitimate spectrum users.”).

V. WIRELESS INTERRUPTIONS IN CORRECTIONAL FACILITIES ARE LEGAL UNDER THE COMMUNICATIONS ACT AND CONSTITUTION

A. Wireless Interruptions by Correctional Facilities Government Actors is Legal under the Communications Act

The prospective interruption of wireless service in the United States has been limited in the past by unduly restrictive interpretations of the Act.¹¹⁹ Section 333 of the Act¹²⁰ is understood to be the major impediment to the deployment of wireless interruption technology, prohibiting devices that “willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications] Act or operated by the United States Government.”¹²¹ Upon detailed examination, this provision of the Act has no applicability to managed access systems used in correctional facilities.

Section 333 proceeded from a series of intentional jamming incidents in which the jammer was using a licensed transmitter, preventing criminal prosecution under Section 301 of the Act.¹²² The Commission sought legislative redress, and Congress responded by affording it “the explicit authority to halt willful or malicious interference”¹²³ Consequently, the use of Section 333 is discretionary, a tool to “assist the Commission in curtailing willful and malicious interference” when it adjudges that such interference proceeded from a “particularly disruptive type of violation.”¹²⁴ Moreover, Section 333 is facially limited to preventing interference with authorized radio *stations*. Wireless interruption in prison focuses on the illegal *use* of such

¹¹⁹ See Section VI.A, *infra*.

¹²⁰ 47 U.S.C. § 333.

¹²¹ Federal Communications Commission Enforcement Bureau, GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions (FAQs), 3 (“Jamming FAQ”), <http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf>.

¹²² 47 U.S.C. § 301 (“No person shall use or operate any apparatus for the transmission of energy or communications or signals by radio . . . except under and in accordance with [the Communications] Act and with a license on that behalf granted under the provisions of this chapter”); see H.R. Rep. No. 316 (1990), *reprinted in* 1990 U.S.C.C.A.N. 1294, 1301-02.

¹²³ S. Rep. No. 101-215 (1989); see Federal Communications Commission Authorization Act of 1990, Pub. L. No. 101-396, 104 Stat. 848 (1990).

¹²⁴ H.R. Rep. No. 316, 1990 U.S.C.C.A.N. at 1302.

stations - the selective block or termination of transmissions sent by inmates who have no entitlement to the possession, much less the operation, of wireless devices. Managed access technology, for example, distinguishes between devices that are utilized in a manner commensurate with prison regulations and those that are not, but does not target the radio station operation in and of itself. No broad, indiscriminate blockage of entire classes of cellular phones or CMRS spectrum allocations occurs, which is the sort of activity that gave rise to Section 333.¹²⁵ Thus, systems that facilitate wireless interruption in correctional facility do not fall within the ambit of Section 333.¹²⁶ As SCDOC noted in its 2009 Petition for Rulemaking, “[t]here is no legitimate use of CMRS spectrum within correction facilities where the possession and use of CMRS equipment is illegal.”¹²⁷ The absurdity of assessing a criminal penalty under Section 333 for interference with mobile devices that prisoners had no right to use in the first place is clear.¹²⁸

Two subsidiary portions of the Act - Sections 301 and 302(b)¹²⁹ - have been used in concert with Section 333 to deter the sale and operation of wireless interruption devices.¹³⁰ Section 301, in pertinent part, prohibits the use or operation of radio devices without a license granted under the Act. Section 302(b) of the Act prohibits, *inter alia*, the manufacture, import, and sale of devices that fail to comply with the Commission’s rules promulgated thereunder.

¹²⁵ See, e.g., *Radar Solutions, Ltd. v. U.S. Federal Communications Commission*, 628 F. Supp. 2d 714 W.D.Tex.,2009 (devices intended to jam and modify all police radar signals); *Amateur Radio Station WA4D*, Michael E. Whatley, 5844 Doris Drive, Alexandria, VA 22311, 7 FCC Rcd 7299 (1992) (signals of amateur radio station that interfered with communications of other amateur operators on 7257 kHz and 7258 kHz via rude and harassing comments), *forfeiture assessed*, 8 F.C.C.R. 5619 (1993); *Cordell Engineering, Inc.*, 14 FCC Rcd 7440 (1992) (interference by amateur radio station with 10-channel trunked specialized mobile radio system).

¹²⁶ Cf. *Bling Wholesalers, et al.*, 26 FCC Rcd 13565, ¶ 9 (2011) (“Signal jammers, however, cannot be certified or authorized because their primary purpose is to block or interfere with authorized radio communications. As noted above, a device intended for such use is clearly prohibited by section 333 of the Communications Act.”).

¹²⁷ SCDOC Petition at 10.

¹²⁸ As GTL noted in its 2011 Petition for Rulemaking, it would be a simple matter for the Commission to make manifest this point by amending 47 C.F.R. § 22.3(b), “so it is clear that where state and local law make CMRS subscriber equipment illegal in corrections facilities, such use is also illegal under federal law.” GTL Petition at 17.

¹²⁹ 47 U.S.C. § 302(b).

¹³⁰ Jamming FAQ at 3.

These regulations include 47 C.F.R. §§ 2.803(a)(1) (barring the marketing of radio frequency devices without Commission certification), 15.201(b) (requiring the certification of intentional radiators), and 15.3(o) (defining “intentional radiator”).¹³¹ Thus, both Section 301 and 302(b), via their attendant regulations, rest on one central point - wireless interruption technology “cannot be certified or authorized because the[ir] main purpose . . . is to block or interfere with radio communications,” pursuant to Section 333.¹³² As already explained, this represents an overbroad reading of Section 333, which prescribes *discretionary* enforcement for devices that interfere with *authorized* radio communication. Absent the Section 333 rationale, there is no reason why wireless interruption technology cannot be used by peace officers to combat illegal cell phone use where such steps are both practical and necessary for the Commission to undertake.

Moreover, several exceptions to Section 302 mean that the manufacture and sale of wireless interruption technology for installation in federally-owned prisons is permitted. 47 U.S.C. § 302(c) provides that Section 302 does not apply to, *inter alia*, “systems for use by the Government of the United States or any agency thereof” while 47 C.F.R. § 2.807(d) excepts “[r]adiofrequency devices for use by the Government of the United States or any agency thereof” from the scope of 47 C.F.R. § 2.803. The Act provides no rationale why these same exceptions should not be extended to state and local departments of corrections, which perform the same kinds of incarceration (and face the same sort of security problems) as their federal analogues.

B. Wireless Interruption is Ripe for Forbearance under the Commission’s Statutory Forbearance Mandate

47 U.S.C. § 160(a) instructs the Commission to “forbear from applying any regulation or any provision of this chapter to a telecommunications carrier or telecommunications service” if

¹³¹ See, e.g., *DealExtreme*, 26 FCC Rcd 1322, ¶ 6 (2011).

¹³² *New Century Technology*, 26 FCC Rcd 388, ¶ 7 (2011).

“(1) enforcement of such regulation or provision is not necessary to ensure that the charges, practices, classifications, or regulations by, for, or in connection with that telecommunications carrier or telecommunications service are just and reasonable and are not unjustly or unreasonably discriminatory; (2) enforcement of such regulation or provision is not necessary for the protection of consumers; and (3) forbearance from applying such provision or regulation is consistent with the public interest.” Congress instituted this statute as part of the Telecommunications Act of 1996¹³³ to “require[]” the Commission to forbear from exercising its regulatory authority if the three-part test is met.¹³⁴ As numerous FCC precedents attest, the language of Section 160(a) and the concomitant legislative intent effectively render this section a Congressional mandate.¹³⁵ While provisions exist enabling a telecommunications carrier, or class of telecommunications carriers, to submit a petition for forbearance,¹³⁶ the Commission may forbear from enforcement of the Act on its own motion when the precepts of 47 U.S.C. §

¹³³ Pub. L. No. 104-104, 110 Stat 56, § 10 (1996).

¹³⁴ H.R. Conf. Rep. No. 104-458 (1996), *reprinted in* 1996 U.S.C.C.A.N. 10, 184-85; *accord* S. Conf. Rep. 104-230 (1996),.

¹³⁵ *See, e.g., Petitions of Qwest Corporation for Forbearance Pursuant to 47 U.S.C. § 160(c) in the Denver, Minneapolis-St. Paul, Phoenix, and Seattle Metropolitan Statistical Areas*, 23 FCC Rcd 11729, n. 95 (2008) (describing Section 160(a) of the Act as a “mandate”); *Petitions of Qwest Corporation for Forbearance Pursuant to 47 U.S.C. § 160(c) in the Boston, New York, Philadelphia, Pittsburgh, Providence and Virginia Beach Metropolitan Statistical Areas*, 22 FCC Rcd 21293, n. 77 (2007) (same); *Petition of ACS of Anchorage, Inc. Pursuant to Section 10 of the Communications Act of 1934, as Amended (47 U.S.C. § 160(c)), for Forbearance from Certain Dominant Carrier Regulation of its Interstate Access Services, and for Forbearance from Title II Regulation of its Broadband Services, in the Anchorage, Alaska, Incumbent Local Exchange Carrier Study Area*, 22 FCC Rcd 16304, ¶ 26 (2007) (same); *In re Verizon*, 18 FCC Rcd 23525, 23534 (2003) (“Congress, giving teeth to its general preference for competition over regulation, not only authorized elimination of a Commission regulation through the vehicle of forbearance, but went so far as to mandate forbearance from any regulation where the three-part set forth in section 10(a) is satisfied. 47 U.S.C. § 160(a).”) (dissenting statement of Commissioner Kathleen Q. Abernathy); *Policy and Rules Concerning the Interstate Interexchange Marketplace*, 14 FCC Rcd 391 (1998) (dissenting statement of Commissioner Michael K. Powell) (Jan . 29, 1999) (“[T]he Commission, in subsections (a) and (b) of Section 10, is directed to ‘determine’ and ‘consider’ certain things and mandates forbearance (‘shall’) if the Commission determines that the three enumerated considerations warrant. 47 U.S.C. § 160(a), (b). These words suggest that the Commission has an affirmative duty to work through, not whether forbearance is warranted, but whether the challenged regulation is warranted any longer. For if it is not, forbearance is mandated as a matter of law.”).

¹³⁶ *See* 47 U.S.C. § 160(c); *see also, e.g., Petitions of Qwest Corporation, supra.*

160(a) are met.¹³⁷

Applying its three-part test, Section 160(a) demands that state and local correctional facilities be afforded the right to rely on their telecommunications service providers to provide wireless interruption systems.¹³⁸ First, curtailment of wireless access for inmates does not affect the economic or legal framework for CMRS service. “Necessary” has been defined by the D.C. Circuit as a “strong connection” between a requirement and a regulatory goal.¹³⁹ There is *no* connection between a clandestine possessor and operator of a wireless device and the economic well-being of a typical CMRS consumer. Forbearance in this context “would not prevent the Commission from enforcing sections 201 or 202 of the Act, which require all carriers to charge just, reasonable, and non-discriminatory rates.”¹⁴⁰ Second, no consumers are aided by withholding wireless interruption systems from prisons. In fact, the converse is true - consumers (or, more accurately, the public at large) are at increasing risk from a paucity of wireless interruption technology, given the dangers inherent when inmates acquire and use wireless devices to facilitate escapes or the commission of crimes. The Commission cannot ignore the ramifications of this calculus, given that “a critical component of the consumer protection goal is the protection of public safety,” one that “Congress has expressly directed the Commission to consider . . . when exercising its regulatory authority.”¹⁴¹ Wireless interruption capability

¹³⁷ See, e.g., *Lifeline and Link Up Reform and Modernization; et al.*, 55 Comm Reg. (P&F) 471, ¶ 368 (2012); *ComTech Petition for Declaratory Ruling that Licensees of Nationwide 220 MHz Mobile Communications Systems are Not Required to License Separately Each of the Systems' Base Stations*, 16 Comm. Reg. (P&F) 987, n. 12 (1999) (forbearing on own motion, and taking no position on whether subject corporation’s petition falls within parameters of 47 U.S.C. § 160(c)).

¹³⁸ Note that 47 U.S.C. § 160(a) requires “no particular mode of market analysis or level of geographic rigor,” such that forbearance is justified even in light of variations amongst correctional facilities. *EarthLink, Inc. v. F.C.C.*, 462 F.3d 1, 8 (D.C. Cir. 2006).

¹³⁹ *Cellular Telecommunications & Internet Association v. F.C.C.*, 330 F.3d 502, 512 (D.C. Cir. 2003); compare, e.g., *Telecommunications Carriers Eligible for Universal Service Support*, 26 FCC Rcd 13723, n. 33 (2011).

¹⁴⁰ *Telecommunications Carriers Eligible for Universal Service Support* ¶ 10.

¹⁴¹ *E911 Accuracy Standards on Tier III Carriers*, 18 FCC Rcd 24648, ¶ 15 (2003); see also *Framework for Broadband Internet Service*, 25 FCC Rcd 7866 (2010) (noting “Commission’s mission with respect to promoting

provided by telecommunications carriers under the auspices of correctional facilities will certainly provide a boon in security and safety to consumers in the aggregate.¹⁴² Finally, public safety, per the integrity of correctional facilities, means that forbearance is entirely in the public interest. As the Commission observed in *Wackenhut Corporation*, the final Section 160(a) criteria is met by “facilitat[ing] operation of a system that enhances safety of the general public located within [a] service area . . . result[ing] in more efficient use of the spectrum.”¹⁴³

Forbearance will permit standardization among and cooperation between federal, state, and local correctional facility administrators. As evinced by statutes governing the Department of Homeland Security (“DHS”), this sort of unified approach is vital in tackling difficult security challenges. 6 U.S.C. § 162(a)(1), for example, instructs the DHS “to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.” According to 6 U.S.C. § 112(c)(1), the DHS Secretary is responsible for “coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities.” Other examples evince a similar intent.¹⁴⁴ It is incumbent upon the Commission to adopt a similar mode of integrated nationwide leadership, per its role in

safety of life and property, and consumer protection generally”); *Keller Communications, Inc. v. F.C.C.*, 130 F.3d 1073, 1076-77 (D.C. Cir. 1997) (affirming Congressional direction to consider public safety needs).

¹⁴² Cf. *Telecommunications Carriers Eligible for Universal Service Support; Federal-State Joint Board on Universal Service*, 25 FCC Rcd 10510, ¶ 10 (2010) (providing certification conditions to maximize consumer protection in regard to non-facilities based Lifeline Eligible Telecommunications Carriers).

¹⁴³ 13 FCC Rcd 16810, ¶ 7 (1998).

¹⁴⁴ See, e.g., 6 U.S.C. § 182(6) (designating DHS Secretary as responsible for “establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities”); 6 U.S.C. § 361 (establishing Office for State and Local Government Coordination, which shall “(1) coordinate the activities of the Department relating to State and local government; (2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism; (3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and (4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities”).

promoting the safety of life and property through radio communication.¹⁴⁵

C. The First Amendment Does Not Prohibit Wireless Interruptions in Prisons

The Commission's concerns over the First Amendment implications of wireless service interruption are moderated in regard to a prison, which is "most emphatically not a 'public forum'" for purposes of free speech.¹⁴⁶ Far from designating a correctional facility as an institution open to assembly and debate, the "policy and practice" of government authorities has been to limit expressive activities concomitant with security and administrative interests.¹⁴⁷

While an inmate retains his or her First Amendment rights while incarcerated, they are trumped in cases where they are inconsistent with an individual's status as a prisoner, or with the legitimate penological objectives of the corrections system.¹⁴⁸ "[M]aintaining institutional security and preserving internal order and discipline are essential goals that may require limitation or retraction of the retained constitutional rights of both convicted prisoners and pretrial detainees," such that "even when an institutional restriction infringes a specific constitutional guarantee, such as the First Amendment, the practice must be evaluated in the light

¹⁴⁵ 47 U.S.C. § 151; see, e.g., *Remington Arms Company, Inc. Request for a Waiver of the Part 15 Regulations*, 20 FCC Rcd 18724 (2005). *Remington Arms* granted a waiver of Commission rules governing digital modulation requirements and power spectral density limits to facilitate the operation of the Eyeball R1 imaging sensor, "intended for counter-terrorism and law enforcement operations in urban terrain applications as well as in police activities requiring observation and surveillance." *Id.* ¶ 2. Remington stated "that its Eyeball R1 transmitter will serve the public interest in saving lives and combating terrorism. Remington states that any possible interference would be limited to other unlicensed devices in the immediate area surrounding the Eyeball R1 and that this area, in many situations, would be evacuated or under police control. Remington adds that the potential for disruption will be of limited duration, is unlikely to recur in the same area or location, will rarely exceed the area of immediate concern to the law enforcement operation . . ." *Id.* ¶ 4. The Commission predicated its waiver on the grounds that the Eyeball R1 would "serve the public interest because law enforcement will be able to use it to help save lives," and would permit "the operation of devices that would provide law enforcement agencies with new technology for investigating hostile situations without endangering police personnel." *Id.* ¶¶ 1, 6.

¹⁴⁶ *Jones v. North Carolina Prisoners' Labor Union, Inc.*, 433 U.S. 119, 136 (1977).

¹⁴⁷ *Cornelius v. NAACP Legal Defense and Education Fund*, 473 U.S. 788, 802 (1985); cf. *Turner v. Safley*, 482 U.S. 78, 89 (1987) ("[W]hen a prison regulation impinges on inmates' constitutional rights, the regulation is valid if it is reasonably related to legitimate penological interests. . . . Subjecting the day-to-day judgments of prison officials to an inflexible strict scrutiny analysis would seriously hamper their ability to anticipate security problems and to adopt innovative solutions to the intractable problems of prison administration").

¹⁴⁸ See, e.g., *Clement v. California Department of Corrections*, 364 F.3d 1148, 1151 (9th Cir. 2004); *Lindell v. Frank*, 377 F.3d 655, 657 (7th Cir. 2004).

of the central objective of prison administration, safeguarding institutional security.”¹⁴⁹

Accordingly, an inmate’s right to communicate with family and friends may be curtailed upon “a showing of a substantial governmental interest serving the legitimate and reasonable needs and exigencies of the institutional environment.”¹⁵⁰

Courts have repeatedly ruled that the mere *possession* of wireless devices, per the threat they pose to the safety, security, and goals of correctional institutions, is subject to summary discipline. In *People v. Green*, the Sullivan County Court held “that as a matter of law a cell phone, no matter how a defendant may use it, is inherently DANGEROUS because a cell phone or other telecommunication device has a substantial probability that the item itself may be used in a manner that is likely to bring out major threats to a detention facility's institutional safety or security by the defendant, or other inmates, in the facility.”¹⁵¹ A felony conviction for attempted provision of cellular phones to inmates was upheld in *Murrell v. State*, per the court’s determination that “[t]he presence of cellular telephones in a prison undermines discipline and can facilitate other misconduct,” as “inmates with cellular telephones can direct criminal activity from behind bars, thereby defeating the purpose of removing convicted criminals from society to serve their sentences.”¹⁵² In *Materon v. Ebbert*, the Third Circuit affirmed a disciplinary conviction on the grounds that an inmate’s cell phone constituted a “hazardous tool,” one that might be used to arrange a rendezvous for an escape attempt to facilitate trafficking in contraband goods.¹⁵³ Numerous other cases have reached similar conclusions.¹⁵⁴ As the

¹⁴⁹ *Bell v. Wolfish*, 441 U.S. 520, 547 (1979). .

¹⁵⁰ *Morgan v. LaVallee*, 526 F.2d 221, 225 (2d. Cir. 1975).

¹⁵¹ 927 N.Y.S.2d 296, 302 (2011).

¹⁵² 960 N.E.2d 854, 859 (Ind. Ct. App. 2012) (“Based on these considerations, we cannot conclude that Murrell's punishment for a Class C felony is disproportionate merely because trafficking in cellular telephones is treated similarly to trafficking in controlled substances and weapons.”).

¹⁵³ 446 Fed. Appx. 405 (3rd Cir. 2011); *cf. Garcia v. Zickefoose*, Civil No. 10–1725, 2011 WL 6179785, *11 (D.N.J. Dec. 12, 2011) (“[T]he mere act of possessing and using the cell phones in prison . . . sufficient in satisfying

Supreme Court has held, First Amendment rights do not attach to the dissemination of materials that “create an intolerable risk of disorder” (a lesser standard than materials that are “‘likely’ to lead to violence”),¹⁵⁵ it logically follows that such rights would certainly not attach to inherently dangerous wireless devices *already* in the hands of inmates.

The lawfulness of technology like managed access is buttressed by existing limitations on inmate communication. An inmate has no right to unlimited telephone use, as telephonic communication is “subject to rational limitations in the face of legitimate security interests of the penal institution.”¹⁵⁶ Inmate telephone service is determined by prison administrators, with court oversight applicable only in instances of unreasonable restriction.¹⁵⁷ The Ninth Circuit has disclaimed “any expectation of privacy in outbound calls from prison” as “not objectively reasonable”¹⁵⁸ Accordingly, routine and random monitoring of inmates’ personal phone calls has been upheld by numerous courts,¹⁵⁹ particularly in instances in which notices in this regard have been disseminated.¹⁶⁰ An inmate consents to call monitoring and recording simply by using a telephone.¹⁶¹ Limited calling lists have also been endorsed per the “valid and rational” aim of reducing criminal activity and harassment conducted through telephonic means,¹⁶² especially in light of alternative means of communication.¹⁶³

the evidentiary standard required by due process in prison disciplinary proceedings,” given their propensity for facilitating misconduct”).

¹⁵⁴ See, e.g., *Myrieckes v. Caraway*, Civil Action No. L-11-917, 2012 WL 527585 (D. Md. Feb. 16, 2012); *Malone v. Caruso*, No. 2:09-cv-260, 2011 WL 806617, *1, *3 (W.D. Mich. Mar. 2, 2011); *McMullen v. Director, TDCJ-CID*, No. 6:09cv426, 2011 WL 1113500, *5 (E.D. Tex. Feb. 18, 2011); *Kalasho v. Martin*, No. Civ.A.02CV71854-DT, 2005 WL 1355065, *5 (E.D. Mich. Mar. 25, 2005).

¹⁵⁵ *Thornburgh v. Abbott*, 490 U.S. 401, 417 (1989).

¹⁵⁶ *Strandberg v. City of Helena*, 791 F.2d 744, 747 (9th Cir. 1986) (internal quotation marks omitted).

¹⁵⁷ *Washington v. Reno*, 35 F.3d 1093, 1100 (6th Cir. 1994).

¹⁵⁸ *U.S. v. Van Poyck*, 77 F.3d 285, 291 (9th Cir. 1996).

¹⁵⁹ See, e.g., *U.S. v. Lewis*, 406 F.3d 11 (1st Cir. 2005); *U.S. v. Vasta*, 649 F. Supp. 974 (S.D.N.Y. 1986); *Crooker v. U.S. Dept. of Justice*, 497 F. Supp. 500 (D.C. Conn. 1980).

¹⁶⁰ See, e.g., *U.S. v. Habben*, 258 Fed. Appx. 972 (9th Cir. 2007), *cert. denied*, 552 U.S. 1218 (2008); *U.S. v. Workman*, 80 F.3d 688 (2nd Cir. 1996); *U.S. v. Paul*, 614 F.2d 115 (6th Cir. 1980).

¹⁶¹ See, e.g., *U.S. v. Footman*, 215 F.3d 145 (1st Cir. 2000).

¹⁶² *Pope v. Hightower*, 101 F.3d 1382, 1385.

Nor do visitors to a correctional facility enjoy an untrammelled right to communication, as prisons are inherently institutions where public access is limited.¹⁶⁴ While the specificity of managed access systems moderates its effect on non-incarcerated individuals within prison walls, the fact remains that friends and family may expect no absolute right to speech. In *Lloyd Corp., Ltd. v. Tanner*, the Supreme Court ruled that property does not lose its private character simply because the public is invited to use it for specific purposes.¹⁶⁵ Prison administrators “are to take all necessary steps to ensure the safety of not only the prison staff and administrative personnel, but also visitors.”¹⁶⁶ Such steps may embrace monitoring, with cases like *U.S. v. Peoples* establishing that a discussion between a visitor and inmate through an entirely internal telephone system was subject to monitoring and recording.¹⁶⁷

It should also be noted that depriving inmates of access to and use of wireless devices does not eliminate all methods of communication.¹⁶⁸ In addition to handwritten letters and visits from family and friends, prisoners may still use designated inmate calling systems. Such wireline alternatives, pioneered by companies like GTL, provide correctional facility administrators with the ability to monitor and record calls, and limit communications based on individual disciplinary records and the time of day. As long as these kinds of “reasonable and effective means of communication remain open and no discrimination in terms of content is involved,” prison officials must be afforded substantial “latitude” in curtailing inmates’ First

¹⁶³ *Id.* (“The undisputed evidence establishes that Pope had alternate means of exercising this right because he could receive visitors and correspond with virtually anyone he wished.”).

¹⁶⁴ *Saxbe v. Washington Post Co.*, 417 U.S. 843, 849 (D.C. Colo. 1974); see *Adderley v. State of Florida*, 385 U.S. 39, 41 (1966) (“Traditionally, state capitol grounds are open to the public. Jails, built for security purposes, are not.”).

¹⁶⁵ *Lloyd Corp., Ltd. v. Tanner*, 407 U.S. 551, 569-70 (1972) (“Few would argue that a free-standing store, with abutting parking space for customers, assumes significant public attributes merely because the public is invited to shop there.”).

¹⁶⁶ *Hudson*, 468 U.S. at 526.

¹⁶⁷ 250 F.3d 630 (8th Cir. 2001); see, e.g., *Christman v. Skinner*, 468 F.2d 723, 726 (2nd Cir. 1972).

¹⁶⁸ See *Overton v. Bazzetta*, 539 U.S. 126, 135 (2003) (“Were it shown that no alternative means of communication existed, though it would not be conclusive, it would be some evidence that the regulations were unreasonable.”).

Amendment rights vis-à-vis limitations on wireless communication.¹⁶⁹ Closing one channel of expression does not render those that remain open “illusory”¹⁷⁰ or unacceptable because they do not represent the “ideal” mode of communication.¹⁷¹ Given the grave security concerns posed by illegal wireless devices in prison and the alternative avenues of communication that are available, the argument that a prisoner has a First Amendment right to make a phone call on an illegal contraband cell phone cannot be seriously entertained. It would be akin to arguing that freedom of worship permits religious clothing to be worn outside divine services, despite the fact that such clothing could conceal shanks and razor blades,¹⁷² or the right to read freely permits the receipt of books from sources other than bookstores or publishers, when such books could easily be hollowed out for the transport of contraband.¹⁷³

As a rule, inmates bear the burden of disproving the validity of prison regulations.¹⁷⁴ Managed access systems, borne from exigency, rather than convenience, are a proven tool to curb the growing problem of wireless usage in prisons that facilitates a host of crimes. They do not interfere with existing inmate telephone calling systems, and do not deprive prisoners of communication via post or visit. They meet the needs of prison populations where inherently illegal wireless devices are commonplace, and follow on failed attempts to restore order through

¹⁶⁹ *Pell v. Procunier*, 417 U.S. 817, 826 (1974) (internal quotation marks omitted).

¹⁷⁰ *Woods v. Commissioner of the Indiana Dep’t of Corrections*, 652 F.3d 745, 749 (7th Cir. 2011) (dismissing inmates’ First Amendment challenge based on regulation barring access to online pen-pal sites).

¹⁷¹ *Overton*, 539 U.S. at 135 (“Alternatives to visitation need not be ideal, however; they need only be available.”).

¹⁷² *See, e.g., Muhammad v. Lynaugh*, 966 F.2d 901, 902-03 (5th Cir. 1992) (“Allowing inmates to wear these religious articles in other areas conceivably could undermine the [Texas Department of Criminal Justice]’s legitimate penological interests, primarily its overriding concern for prison security.”).

¹⁷³ *Bell*, 441 U.S. at 548-52 (noting existence of, *inter alia*, prison library as alternative source of reading material).

¹⁷⁴ *See, e.g., Jones*, 433 U.S. at 128. *see also, Turner v. Safley*, 482 U.S. 78 (1987) (outlining four-part test for evaluating the reasonableness of restricting a constitutional right vis-à-vis legitimate penological interests: (1) whether there is a “valid, rational connection” between the regulation and a legitimate governmental interest put forward to justify it; (2) whether there are alternative means of exercising the asserted constitutional right that remain open to the inmates; (3) whether and the extent to which accommodation of the asserted right will have an impact on prison staff, inmates, and the allocation of prison resources generally; and (4) whether the regulation represents an “exaggerated response” to prison concerns. (*citing, Pope*, 101 F.3d at 1384)).

the use of inmate searches and penalty assessments. Their largely transparent operation frees prison resources following installation, freeing officials from performing more (and often fruitless) cell-by-cell search and retrieval operations. Distinguishing only between “authorized” and “unauthorized” calls, they foster no distinctions between individual prisoners, and are not subject to the discretion of individual correctional officers. Given that there exists no technology that would fully accommodate free speech rights in prison “at a de minimis cost to valid penological interests,” and because no valid alternatives are evident, First Amendment concerns surrounding the introduction of managed access technology are marginal at best.¹⁷⁵

VI. CORRECTIONAL FACILITIES, AS GOVERNMENT ACTORS, MUST BE AUTHORIZED TO RELY ON WIRELESS INTERRUPTIONS TO ADDRESS UNLAWFUL CELL PHONE USE

At its most basic level, wireless service interruption constitutes another tool for the oversight of inmates and the safety of correctional facilities. While more complex than other security systems, like cameras or metal detectors, the purpose is the same - to deter the introduction and prevent the use of a dangerous tool amongst prisoners. To that specific end, correctional facility administrators are well equipped to oversee the deployment or use of such technology by their telecommunications service providers for integration with existing prison police and protection methods. This is especially true in the context of managed access systems, where the architecture and requirements of individual prisons dictate implementation and

¹⁷⁵ Cf., e.g., *Price v. New York City Bd. of Education*, 51 A.D.3d 277, 287 (N.Y. App. Div. 2008), *leave to appeal denied*, 894 N.E.2d 653 (2008). In *Price*, the New York Appellate Division upheld the right of a school chancellor to institute a complete cellular phone use ban on campus. Observing the “now routine” requests that theater and movie patrons turn off such devices, the court reasoned that “it was not unreasonable for the Chancellor to recognize that if adults cannot be fully trusted to practice proper cell phone etiquette, then neither can children.” The court further disclaimed analogies to school dress regulations as “strained,” noting that while “a ban on hats in the classroom is easily enforced, without a need to extend it elsewhere. . . . a ban on possession on cell phones is necessary because a ban on use is not easily enforced.” Overall, *Price* concluded, “it cannot be denied that the use of cell phones for cheating, sexual harassment, prank calls and intimidation threatens order in the schools.”

functionality.¹⁷⁶

Correctional facilities are, “by definition . . . places of involuntary confinement of persons who have a demonstrated proclivity for antisocial criminal, and often violent, conduct.”¹⁷⁷ Officials are therefore bound to “to take reasonable measures to guarantee the safety of the inmates themselves. They must be ever alert to attempts to introduce drugs and other contraband into the premises which . . . is one of the most perplexing problems of prisons today; they must prevent, so far as possible, the flow of illicit weapons into the prison; they must be vigilant to detect escape plots, in which drugs or weapons may be involved, before the schemes materialize.”¹⁷⁸ In light of this “extraordinarily difficult task” that faces prison administrators, and by dint of long experience, courts have entrusted them to enact security and methods in measured fashion.¹⁷⁹ In assessing the ramifications of facilitating wireless interruption in prisons, and the extent to which prison administrators should be entrusted to do so in a responsible way, the Commission should bear in mind the words of the Supreme Court: administrators “should be accorded wide-ranging deference in the adoption and execution of policies and practices that in their judgment are needed to preserve internal order and discipline and to maintain institutional security.”¹⁸⁰ Such deference has been understood to encompass not merely the response to an active disturbance, but the “prophylactic measures to prevent such a disturbance.”¹⁸¹ The Commission itself is cognizant of this fact, having observed over fifteen years ago that “corrections officials . . . have broad discretion in deciding whether to permit inmate calling, [and] may restrict inmate calling for reasons of security, discipline, or fraud

¹⁷⁶ See, e.g., California IFB.

¹⁷⁷ *Hudson v. Palmer*, 468 U.S. 517, 526 (1984).

¹⁷⁸ *Id.* at 526-27.

¹⁷⁹ *Id.* at 527 (internal quotation marks omitted).

¹⁸⁰ *Bell*, 441 U.S. at 547.

¹⁸¹ *Jeffers v. Gomez*, 267 F.3d 895, 917 (9th Cir. 2001).

prevention.”¹⁸²

A timely and economical “prophylactic measure” for immediate managed access implementation is the extension of the PROTECT Initiative global carrier database to correctional facilities.¹⁸³ Providers of telecommunications services to correctional facilities can identify the International Mobile Equipment Identity (“IMEI”) associated with each mobile device unlawfully used in a prison. The IMEI is a 15-digit number that is used to identify the device when it is used on a mobile phone network.¹⁸⁴ Once intercepted, this information in turn can be communicated to the PROTECT database administrator for immediate deactivation of the phone by the appropriate CMRS provider.¹⁸⁵ The prompt deactivation of illegal devices will also obviate the need for time-consuming cell-by cell searches. Most importantly, the original intent of the PROTECT Initiative - to increase public safety by removing the link between stolen wireless devices and profitability - is augmented and enhanced.

While the use of the PROTECT Initiative will serve as an excellent immediate managed access solution, its effectiveness will be tested by time and resourcefulness of inmates and their outside confederates. Thus, long-term security of correctional facilities may require more immediate and direct interruption of any wireless transmission initiated by a prisoner, as even one completed call may be sufficient to facilitate violence or murder. This may necessitate the introduction of devices into prisons that specifically facilitate wireless interruption without the

¹⁸² *Petition for Declaratory Ruling by the Inmate Calling Services Providers Task Force*, 11 FCC Rcd 7362, ¶ 31 (1996).

¹⁸³ See attached Affidavit of Joseph S. Noonan on behalf of Global Tel*Link Corporation (Apr. 25, 2012) (“Noonan Affidavit”).

¹⁸⁴ *Id.* ¶ 2. The GSMA maintains a unique system known as the IMEI Database (IMEI DB), which is a global central database containing basic information on serial number (IMEI) ranges of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) that are in use across the world’s mobile networks. The IMEI DB also supports what is known as a “black list”. The black list is a list of IMEIs that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. See www.gsma.com/imei-database/.

¹⁸⁵ Noonan Affidavit ¶ 3.

delay of waiting for wireless carrier response based on an information exchange between correctional facilities and the PROTECT database.

As GTL explained in its Petition for Rulemaking last year, the Commission can play a critical role in overseeing the deployment of such wireless interruption technology.¹⁸⁶ Through judicious application of existing or enhanced standards promulgated by the Office of Engineering and Technology, the Commission can ensure that any system will be installed and operated in the public interest. Permitting entities with no known qualifications to interact with telecommunications service providers or law enforcement agencies, to install and operate sensitive telecommunications infrastructure, borders on the reckless and irresponsible. To this end, the FCC can require that entities seeking to deploy a wireless interruption system must provide their services through an authorized provider of telecommunications services selected by the correctional facility. Such authorizations carry with them financial and technical evaluations, and provide wireless consumers with points of contact for regulatory redress. Coordination with law enforcement and correctional officers - of the sort pursued in the Maryland, Mississippi, and South Carolina tests - should also be required, culminating in written approval from the institution administrator and a contract with the correctional facility. Much of the groundwork for such authorization has already been established in the Experimental Radio Licenses¹⁸⁷ and Special Temporary Authorizations¹⁸⁸ granted for wireless interruption tests in prisons. Most

¹⁸⁶ See, e.g., NTIA Report at 25 (“Coordination of spectrum issues between the FCC, the wireless carriers, and the managed access provider is critical for successful implementation.”).

¹⁸⁷ See, e.g., Office of Engineering and Technology File No. 0202-EX-PL-2009, Tecore, Inc. Application for New or Modified Radio Station under Part 5 of FCC Rules - Experimental Radio Service (Other Than Broadcast) (2009) (application containing detailed testing parameters and geographical limits, along with CTIA support letter and carrier consent letter); Office of Engineering and Technology File No. 0355-EX-PL-2010, Tecore, Inc. Application for New or Modified Radio Station under Part 5 of FCC Rules - Experimental Radio Service (Other Than Broadcast) (2010) (application containing detailed Experimentation Description describing “minimal and manageable area of interference potential” pursuant to proposed test).

¹⁸⁸ See, e.g., Special Temporary Authorization File Nos. 0004344567, 0004345516, 0004345517, 0004345518, 0004345519, 0004345520, 0004345521, Tecore Government Services LLC, Certification (2010) (applications for

importantly, the Commission can ensure the cooperation of all CMRS carriers, per the public interest obligations that proceed from their licenses, in facilitating the wireless interruption and deactivation of illegal devices in the nation's prisons.

CONCLUSION

More than thirty years ago, the Supreme Court deemed it to be “obvious and unarguable that no governmental interest is more compelling than the security of the Nation.”¹⁸⁹ The growing trend of inmate use of wireless devices portends no less than a security crisis in this country's prisons. It is incumbent upon the Commission - in concert with existing domestic and foreign practices and backed by clear legal precedent - to address this matter in an expeditious fashion. The use of the PROTECT Initiative's global carrier database should be immediately extended to correctional facilities, to deter the proliferation of wireless devices amongst prisoners. In the long term, as protection of the public requires, more direct wireless interruption

spectrum leasing arrangements containing detailed testing parameters and geographical limits, Regulatory Certification, and Description of Requirement).

¹⁸⁹ *Haig v. Agee*, 453 U.S. 280, 307 (1981) (internal quotations marks omitted).

technology may be deemed necessary to comprehensively restore order and safety in prisons. In either event, as demonstrated in these Comments, there exists no technical, legal, or operational rationale for withholding this critical capability from our nation's embattled correctional facilities.

Respectfully submitted,

GLOBAL TEL*LINK CORPORATION

/s/ Chérie R. Kiser

Chérie R. Kiser

Matthew L. Conaty*

Cahill, Gordon & Reindel LLP

1990 K Street, NW, Suite 950

Washington, D.C. 20006

202-862-8900 (telephone)

866-255-0185 (facsimile)

ckiser@cahill.com

Dated: April 30, 2012

* Admitted in NY only.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

**Commission Seeks Comments on Certain
Wireless Service Interruptions**

)
) GN Docket No. 12-52
)
)

**AFFIDAVIT OF JOSEPH S. NOONAN
ON BEHALF OF GLOBAL TEL*LINK CORPORATION**

Joseph S. Noonan, being first duly sworn, upon his oath deposes and states as follows:

1. My name is Joseph S. Noonan. I am the CEO for Corrections.com. In this capacity, I am familiar with the operation of wireless devices and their use in correctional facilities. The facts stated herein are within my personal knowledge.

2. An International Mobile Equipment Identity (“IMEI”) is a 15-digit number used to identify wireless devices when they are used on a mobile phone network. All mobile phones have a unique IMEI.

3. When an unlawful wireless call is made from a correctional facility, the telecommunications service provider serving that facility can capture the associated IMEI. This IMEI can then be communicated by the telecommunications service provider via the PROTECT Initiative database, or similar shared mobile phone identification database, to the appropriate commercial mobile radio service (“CMRS”) provider. The CMRS provider can then use this IMEI to immediately deactivate the illicit wireless device.

I declare under penalty of perjury that the statements in the foregoing are true and correct to the best of my knowledge and belief.

DATED: April 25, 2012



Joseph S. Noonan, CEO
Corrections.com