

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)
)
Promoting Technological Solutions to Combat) GN Docket No. 13-111
Contraband Wireless Device Use in Correctional)
Facilities)

To: The Commission

REPLY COMMENTS OF T-MOBILE USA, INC.

Steve Sharkey
Eric Hagerson

T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004
(202) 654-5900

July 17, 2017

TABLE OF CONTENTS

Introduction and Summary	1
Discussion	3
I. The Record Demonstrates that a Rule Requiring CMRS Carriers to Disable Wireless Devices in Correctional Facilities is Unnecessary	3
II. Any New Rules Must Be Technically Feasible	4
A. Quiet Zones Are Not a Viable Solution to the Contraband Phone Problem	4
B. It Is Not Technically Feasible to Leverage CMRS Networks as a Solution	5
III. The Commission Should Not Require Jamming or Implementation of Proprietary Solutions	6
A. The Communications Act Precludes Jamming as a Solution	6
B. Commenters Oppose Any Rules Promoting the Deployment of Proprietary Beacon Technology	7
IV. Any New Rules Should be Limited to Disabling Wireless Service and Not Require Fully Disabling All Device Software and Functionality	8
A. The Record Is Not Well-Developed Regarding Disabling Devices, and Many Policy Considerations Still Need to be Fully Vetted	8
B. There Are Serious Questions About the Feasibility of Fully Disabling Devices	11
V. If Carriers are Required to Terminate Service, Certain Protections Must Be Incorporated into the Rules	13
A. Service Should Only Be Terminated Pursuant to a Court Order	14
B. CMRS Carriers Must Be Granted Liability Protection	15
C. CMRS Carriers Must Be Entitled to Recover Costs Associated with Compliance	15
VI. The Record Demonstrates Opposition to Prior Notification Requirements	15
Conclusion	16

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)
)
Promoting Technological Solutions to Combat) GN Docket No. 13-111
Contraband Wireless Device Use in Correctional)
Facilities)

To: The Commission

REPLY COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. (“T-Mobile”)¹ hereby responds to initial comments on the Federal Communications Commission’s (“Commission’s”) Further Notice of Proposed Rulemaking (“*FNPRM*”) about combating contraband wireless devices in correctional facilities.²

INTRODUCTION AND SUMMARY

T-Mobile continues to support efforts to prevent the proliferation and use of contraband wireless devices in correctional facilities. The record demonstrates that effective Contraband Interdiction Systems (“CIS”), such as managed access solutions (“MAS”), are both (1) currently available to correctional facilities, and (2) have already been successfully deployed. Additionally, initial comments provide substantial evidence that carriers are already working hand-in-hand with legitimate CIS providers to help solve the contraband phone problem. Given these realities – and recent Commission efforts to streamline CIS deployment – there is no need to adopt new rules at this time, particularly intrusive and burdensome rules requiring commercial mobile radio service (“CMRS”) carriers to terminate service to alleged contraband devices.

¹ T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

² *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017) (“*R&O*” or “*FNPRM*”).

Rather than adopt new rules, the Commission should allow all interested stakeholders to gain experience with the recently adopted rules designed to facilitate the deployment of CIS prior to deciding whether or not to evaluate if additional rules are necessary.

If the Commission nevertheless promulgates new rules, they must be technically feasible. In this regard, a range of commenters echo T-Mobile's concerns regarding the use of quiet zones and CMRS network-based solutions. These proposals are technically infeasible and should not be adopted. The record also includes strong opposition to any rules that would require jamming or promote proprietary, untested solutions (such as beacon technologies).

Furthermore, any new rules should focus on terminating service and not on disabling the device. Proposals to disable devices are new, and the record has not been sufficiently developed so as to address them. Many practical and policy considerations still need to be fully examined. There are also serious questions about the technical feasibility of fully disabling mobile devices.

Additionally, if new rules requiring CMRS carriers to take actions to terminate service are adopted, the record demonstrates that certain protections are necessary. Specifically, the record reflects that: (1) a secure procedure must be implemented to ensure that service to legitimate customers is not impacted and to prevent fraud and abuse; (2) a court order and/or judicial review must be central to this process; and (3) CMRS carriers should be granted liability protection and allowed to recover all costs associated with complying with the new rules.

Finally, the record shows wide agreement among the wireless industry that requiring CMRS carriers to provide advance notification to CIS providers of network and frequency changes are unnecessary and would impede carrier network management flexibility, which in turn could delay the deployment of new services and technologies.

DISCUSSION

I. THE RECORD DEMONSTRATES THAT A RULE REQUIRING CMRS CARRIERS TO DISABLE WIRELESS DEVICES IN CORRECTIONAL FACILITIES IS UNNECESSARY

Prior to considering what form potential new contraband regulations might take, a preliminary question must be resolved: Are such rules necessary? The record in this proceeding answers this query with a resounding “no.” As commenters demonstrate, numerous CIS have already been deployed across the country.³ These systems are proving effective at combatting the contraband phone problem. In one state alone, MAS solutions have intercepted nearly 12 million communications attempts from over 75,000 unauthorized wireless devices.⁴ Given the Commission’s recent rule changes to aid in the deployment of these systems, such effectiveness is only likely to increase.⁵

As T-Mobile previously explained, the ongoing and growing success of these systems means that the promulgation of additional rules is unwarranted, and very likely counterproductive.⁶ At a minimum, state and local authorities must be given time to evaluate and deploy CIS under the recently adopted rules before the Commission considers moving

³ See, e.g., Comments of T-Mobile USA, Inc., GN Docket No. 13-111, at 3-4 (filed June 19, 2017) (“T-Mobile Comments”); Comments of AT&T Services, Inc., GN Docket No. 13-111, at 4 (filed June 19, 2017) (“AT&T Comments”) (noting in part that AT&T already “leases its licensed spectrum to CIS vendors,” “works with managed access systems vendors to address technical challenges ... while helping corrections facilities fight this scourge,” and has successfully worked with “more than 30 prisons across 8 states”); Comments of CTIA, GN Docket No. 13-111, at 1 (filed June 19, 2017) (“CTIA Comments”).

⁴ CTIA Comments at 4; see also T-Mobile Comments at 1-4; AT&T Comments at 4.

⁵ See *R&O*, 32 FCC Rcd at 2345 ¶ 20 (wherein the Commission noted that it expects that “the changes adopted in [the *R&O*] will have a real and tangible impact”).

⁶ T-Mobile Comments at 3-4.

forward with additional proposals.⁷ Consistent with evidence-based rulemaking principles,⁸ these thoughtful measures must be given time to take effect before the need for new rules can be evaluated.

II. ANY NEW RULES MUST BE TECHNICALLY FEASIBLE

If new rules are adopted, they must be technically feasible.⁹ The record demonstrates that it is technically infeasible to establish quiet zones and leverage CMRS networks to prevent contraband wireless device operation. Thus, these options should not be mandated by any new rules.

A. QUIET ZONES ARE NOT A VIABLE SOLUTION TO THE CONTRABAND PHONE PROBLEM

The record demonstrates that quiet zones are not a viable solution to the contraband phone problem.¹⁰ As commenters explain, radio frequency propagation characteristics make it fundamentally impossible to carve out precisely prison facilities from coverage without creating much larger coverage holes.¹¹ Indeed, as Verizon notes:

⁷ See, e.g., Comments of Verizon, GN Docket No. 13-111, at 2-4 (filed June 19, 2017) (“Verizon Comments”).

⁸ See, e.g., Remarks of Ajit Pai, Chairman, FCC, at the Hudson Institute: The Importance of Economic Analysis at the FCC (Apr. 5, 2017) (quoting Cass Sunstein’s principle that “it is the duty of regulators to ‘obtain a careful and objective analysis of the anticipated and actual effects of regulations, whether positive or negative. We need to look at evidence and data. We need careful assessments before rules are issued, and we need continuing scrutiny afterwards.’”).

⁹ As the Chairman has wisely noted in other contexts, a “light-touch regulatory approach” that “embraces regulatory humility” is paramount in order to both preserve the market broadly, and to avoid unintended consequences in specific. Ajit Pai, Chairman, FCC, Remarks at the U.S. – India Business Council (Mar. 29, 2017).

¹⁰ See, e.g., T-Mobile Comments at 16; CTIA Comments at 11; Verizon Comments at 3.

¹¹ T-Mobile Comments at 16 (“Given the propagation characteristics of radio frequencies, it is impossible to carve out the specific boundaries of a correctional facility from coverage. To create a ‘quiet zone’ around such facilities, carriers would have to eliminate coverage to a much larger area surrounding the facility to ensure no radio signals reach the correctional facility.”); CTIA Comments at 10-11 (“a quiet zone ... cannot stop at a barbed wire fence”).

The construction of new correctional facilities, or an existing correctional facility's authorization for new quiet zone status within licensees' existing coverage areas, would require that wireless providers either re-design their radio access networks or substantially power down their transmitters. Both options would impose significant costs on licensees and adversely affect the reliability of service to consumers.¹²

Moreover, commenters show that the creation of quiet zones would be particularly problematic in rural and other underserved regions – the very areas that are subject to the Commission's ongoing efforts to extend wireless service.¹³ These zones would also create problems for people who live and work in the vicinity of correctional facilities as well as along heavily traveled roads that pass by.¹⁴

In sum, it is technically infeasible to create quiet zones without exacerbating the digital divide and potentially impeding service in other areas, including high-traffic corridors.

B. IT IS NOT TECHNICALLY FEASIBLE TO LEVERAGE CMRS NETWORKS AS A SOLUTION

The record also demonstrates that it is equally impossible to leverage CMRS networks as a solution to the contraband problem.¹⁵ In particular, CMRS carriers cannot use location information generated by their networks to track precisely their customers and determine, based

¹² Verizon Comments at 12.

¹³ See, e.g., CTIA Comments at 10-11 (noting that “in rural areas, wireless service often is provided via higher power antennas on taller towers that cover great distances, and a network re-design to engineer quiet zones could easily take rural consumers near correctional facilities out of service,” and that “[e]ven in urban areas, quiet zones would have to extend substantially beyond the bounds of the prison property”); Verizon Comments at 12 (noting that “[m]any correctional facilities are in or near urban and suburban areas ... with established coverage and that are the focus of licensees' ongoing network densification and 5G deployment efforts”).

¹⁴ See Verizon Comments at 12; AT&T Comments at 7 n.9.

¹⁵ T-Mobile Comments at 16-18; CTIA Comments at 11-12.

on this location information, whether a wireless device is being operated illegally as contraband.¹⁶ Thus, the approach contemplated in the *FNPRM* is not technically feasible.¹⁷

III. THE COMMISSION SHOULD NOT REQUIRE JAMMING OR IMPLEMENTATION OF PROPRIETARY SOLUTIONS

A. THE COMMUNICATIONS ACT PRECLUDES JAMMING AS A SOLUTION

It is well-established that the Communications Act prohibits the use of jamming devices.¹⁸ As CTIA has noted:

The use of jamming devices by state and local authorities is unlawful under Sections 302a(b) and 333 of the Communications Act and contrary to the public interest could have the unintended consequence of putting outside responders at risk in the event of an emergency, such as a prison riot. For these and other reasons, the Commission has correctly declared that jammers are “inherently unsafe” and “per se illegal because they are designed to compromise the integrity of the nation’s communications infrastructure.” In fact, the Commission has concluded in a string of enforcement decisions that jamming devices cannot even be certified or authorized under the Commission’s rules “because their primary purpose is to block or interfere with authorized radio communications.”¹⁹

Ultimately, jamming is a blunt instrument that fails to distinguish between legitimate and non-legitimate users, and would therefore have detrimental effects on the former. Given the likely

¹⁶ T-Mobile Comments at 16-18 (noting in part that “CMRS carriers do not actively track the precise geolocation of their subscribers,” as well as the possible implications under Section 222); CTIA Comments at 11 (noting that it would be “inappropriate for the government to require that CMRS carriers actively track subscribers’ location information,” and that “9-1-1 location based information is only generated in response to a consumer dialing 9-1-1, which serves as authorization to use location information”).

¹⁷ See *FNPRM*, 32 FCC Rcd 2381-82 ¶¶ 128-29.

¹⁸ Verizon Comments at 11.

¹⁹ Letter from Brian M. Josef, Assistant Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 *et al.* (filed Mar. 16, 2017).

unlawfulness of any jamming-based solution under the Act, T-Mobile agrees with Commissioner O’Rielly that jamming is not a viable solution to the contraband phone problem.²⁰

B. COMMENTERS OPPOSE ANY RULES PROMOTING THE DEPLOYMENT OF PROPRIETARY BEACON TECHNOLOGY

The record contains significant opposition to the proposal put forth by Cell Command (formerly Try Safety First) to require the installation of beacon technology in prisons and its proprietary software in all handsets operating in the U.S.²¹ First, adoption of a rule mandating use of Cell Command’s solution would be inconsistent with the Commission’s long-standing policy against choosing technological winners and losers, and would not promote technological neutrality.²²

Second, because beacon technology requires the installation of particular software on all devices, it would take years to implement.²³ Beacon/proprietary software technology solutions also would not address embedded, legacy devices incapable of their software updates or devices brought in from outside of the U.S.

Third, beacon technology opens up the possibility of abuse. Other entities unaffiliated with correctional institutions could install beacons in locations and thus prevent legitimate use unbeknownst to the subscriber. The very companies lobbying the Commission for technology-specific, self-serving mandates have admitted as much in the past. For instance, Cell Command previously made representations to the federal government that its beacon technology, once

²⁰ *FNPRM*, 32 FCC Rcd at 2435 (statement of Commissioner O’Rielly) (“I do want to make one position crystal clear: no matter how this proceeding moves forward, I will not support or approve of any form of jamming technologies.”).

²¹ T-Mobile Comments at 18-19; CTIA Comments at 9-10; Verizon Comments at 13.

²² See T-Mobile Comments at 18 n.51; see also *FNPRM*, 30 FCC Rcd at 2434-35 (Statement of Commissioner O’Rielly) (“I have concerns ... [about] the possibility that the Commission would mandate beacon technologies, which is not a technology neutral approach”).

²³ Verizon Comments at 13.

“embedded into the firmware as a universal standard for all mobile phone devices,” could prevent legitimate and lawful uses not just in “prisons,” but along “highways,” in “classrooms,” “courtrooms,” “airplanes,” “hospitals,” and even in “churches” and “theatres.”²⁴

Finally, it is far from clear whether the Commission can mandate the use of such technology without additional Congressional legislation.²⁵ As the Commission itself tacitly acknowledges, barring incorporation into the equipment authorization process, legislation is likely required to mandate all carriers and device manufacturers adopt a specific technology.²⁶

Ultimately, there are a number of potential solutions to the contraband wireless device problem – from MAS to paint that is capable of shielding RF signals – and the Commission should not adopt rules promoting any single, proprietary solution.

IV. ANY NEW RULES SHOULD BE LIMITED TO DISABLING WIRELESS SERVICE AND NOT REQUIRE FULLY DISABLING ALL DEVICE SOFTWARE AND FUNCTIONALITY

A. THE RECORD IS NOT WELL-DEVELOPED REGARDING DISABLING DEVICES, AND MANY POLICY CONSIDERATIONS STILL NEED TO BE FULLY VETTED

While T-Mobile believes that no new rules are necessary, if the Commission moves forward with promulgating additional regulations, with proper protections a process for disabling wireless service to a contraband device could work reasonably well. As the *FNPRM* notes, numerous individual state departments of corrections support the Commission’s proposal to mandate termination of service to contraband wireless devices.²⁷ While there are some

²⁴ Try Safety First, Inc., White Paper (2010), available at <https://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/White%20Paper%20for%20NTIA%20-%20PDF.pdf>.

²⁵ CTIA Comments at 10.

²⁶ See *FNPRM*, 32 FCC Rcd at 2383 ¶ 131.

²⁷ *Id.* at 2370 ¶ 89.

limitations, for example, some devices may “clone” the unique ID of a valid device and thereby evade detection as a contraband device, CMRS carriers today have the capability to terminate wireless service to a particular device identified by its unique device identifier.

For the first time, the *FNPRM* also raises the prospect that carriers would be required to fully disable devices identified by CIS technologies – presumably meaning disabling not only the device’s access to wireless carrier services but its ability to carry out any other functions at all, whether to run apps, take photos, or connect to Wi-Fi networks.²⁸ Requiring such full disabling of phones would be premature, as there are numerous considerations the Commission should examine further, including the impacts on 911 services, data security, privacy, and civil liberties.

To begin, the *FNPRM* notes that a disabled phone would not have the capability to call 911, whereas a service terminated device would maintain 911 calling capability.²⁹ The Commission should first address whether to sunset the current rules requiring 911 capabilities for non-service initiated (“NSI”) devices before concluding whether to require full device disabling here.³⁰ And there may be good policy reasons to allow 911 calling capabilities to remain, e.g., allowing emergency calling for a device that was misidentified as contraband or use by a prison security guard who was met with violence when confiscating a contraband phone.

²⁸ *Id.* at 2372 ¶ 95 (“As discussed below, we seek to ensure that any disabling process will completely disable the contraband device itself and render it unusable, not simply terminate service to the device as the Commission had originally proposed in the *Notice*.”).

²⁹ Although the *FNPRM* notes that a disabled phone would not have the capability to call 911, the Commission’s rules currently require carriers to permit service-terminated devices to reach emergency personnel via 911 calling. *Id.* at 2375 ¶ 104. Therefore, the Commission should first address whether to sunset the current rules requiring 911 capabilities for non-service initiated (“NSI”) devices before concluding whether to require full device disabling here.

³⁰ *Id.* at 2375 ¶ 104; *see id.* at 2354 ¶ 46 n.152 (referencing *911 Call-Forwarding Requirements for Non-Service Initialized Phones*, Notice of Proposed Rulemaking, 30 FCC Rcd 3449 (2015)).

Additionally, the Commission should seek input from data security professionals on the implications of installing capabilities on devices which can be used (or exploited) remotely, by a party other than the authorized owner, to disable a device. Currently, carriers do support tools that device owners can use to disable and remote wipe their own phones.³¹ But these tools are designed to be used only by authenticated owners of the devices – and thus protections exist against malicious or unauthorized use. Here, the proposal is for a distinct functionality that would circumvent protections an owner put in place to prevent unauthorized disabling of a device.

Many observers have noted that remote capabilities to override security protections can create significant risks to consumers, as the capabilities can be exploited by legitimate parties for illegitimate uses, and can fall into the hands of bad actors.³² Especially in the context of encryption protections, these policy debates have gone on for decades, with contentious views on both sides and at the highest levels of government.³³ Even if one finds significant value in full disabling of contraband devices, it is essential the Commission address fully these concerns, given that misuse could result in service interruptions (including potential interruption of 911

³¹ *Smartphone Anti-Theft Voluntary Commitment*, CTIA, <https://www.ctia.org/initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment> (last visited July 13, 2017).

³² See, e.g., CTIA Comments at 6-7 (noting that any full disablement would “create[] other risks including expanded cybersecurity threats as [any] ‘shut down’ mechanism would be available to hackers,” too).

³³ See, e.g., Stephen Levy, *The Battle over the Clipper Chip*, N.Y. Times (June 12, 1994) <http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>; *Answers to Your Questions About Apple and Security*, Apple, <https://www.apple.com/customer-letter/answers/> (last visited June 13, 2017) (Apple’s FAQ on its objection to government order mandating creation of encryption bypass tools); Jack Detsch, *What Presidential Candidates Are Saying About the Apple v. FBI Debate*, Christian Science Monitor (Feb 19, 2016), <http://www.csmonitor.com/World/Passcode/2016/0219/What-presidential-candidates-are-saying-about-the-Apple-v.-FBI-debate>.

services) for lawful users,³⁴ and would be highly attractive to purveyors of “ransomware” schemes.³⁵

There are also meaningful questions as to whether and how such capabilities, once created, would be subject to oversight such that they are not misused outside of the context of contraband phones, in areas where the legality of third party remote disabling is more contentious and the impact on civil liberties less well supported by law and policy. For example, the Commission has addressed network shutdowns in local transportation systems and, as CTIA noted at the time, the preferable approach for such operations is through an established, centrally coordinated authority and protocol.³⁶ Tools to enable third parties to remotely disable complete functionality of wireless devices require careful consideration about accurate identification of devices to be disabled, and would need further thought to preventing proliferation outside of the established protocol.

B. THERE ARE SERIOUS QUESTIONS ABOUT THE FEASIBILITY OF FULLY DISABLING DEVICES

There are also practical and technical reasons not to adopt a full disabling mandate. Presently, no technical method exists today to implement such a broad disabling rule. To do so

³⁴ The Commission, along with the Federal Trade Commission, has recently taken steps to inquire about practices for addressing security vulnerabilities in wireless devices. *See* Press Release, FCC, FCC Wireless Telecommunications Bureau Launches Inquiry into Mobile Device Security Updates (May 19, 2016), <https://www.fcc.gov/document/fcc-launches-inquiry-mobile-device-security-updates>; Press Release, FTC, FTC To Study Mobile Device Industry’s Security Update Practices (May 19, 2016), <https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices>. Withholding a mandate to require full disabling of contraband devices would be consistent with the policy goals indicated here: to improve wireless device security.

³⁵ *See, e.g.,* Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week’s Cyberattack*, Microsoft Official Blog (May 14, 2017), <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack>.

³⁶ Comments of CTIA – The Wireless Association®, GN Docket 12-52 (filed Apr. 30, 2012).

would involve commitments not only from carriers but from manufacturers of operating systems and devices. Among other things, this would involve careful consideration of the Commission's legal authority to require such design, development, testing, and manufacturing commitments.³⁷

Multiple commenters express concern over adoption of a rule requiring CMRS carriers to completely disable an alleged contraband wireless device.³⁸ The record demonstrates that the capabilities for complete device disabling simply do not exist today and cannot be developed quickly, if at all.³⁹ And, even *if* such a hypothetical solution could be developed, it would be unlikely to work on legacy devices.⁴⁰ It would take years to phase out the preexisting handsets that are already in the market,⁴¹ and the correctional facility ecosystem would *still* be unlikely to see an appreciable decrease in contraband devices as a secondary market for legacy devices would likely emerge.

Commenters also correctly note that broad stakeholder input is needed before any rule requiring the complete disabling of a device is adopted – including input from the original equipment manufacturers, the CMRS carriers themselves, and operating system and app

³⁷ As the Commission is aware, its jurisdiction over these entities is more limited than its Title III jurisdiction over wireless carriers.

³⁸ T-Mobile Comments at 2 n.5; CTIA Comments at 6-7 (noting that any full disablement would “create[] other risks including expanded cybersecurity threats as [any] ‘shut down’ mechanism would be available to hackers,” too); Verizon Comments at 8-9 (noting that “[t]o remotely and reliably disable appropriate devices would require extensive development by a number of players in the wireless ecosystem,” and would still “not address the large embedded base of handsets in the marketplace today”).

³⁹ Verizon Comments at 8-10.

⁴⁰ *Id.*

⁴¹ As one commenter notes, the length of such a transition was made apparent to the Commission in transitioning the embedded base of handsets to E-911 location-capable models. *See* Verizon Comments at 10 (citing *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Fourth Memorandum Opinion and Order, 15 FCC Rcd 17442 (2000)).

developers, among others.⁴² This is especially critical in light of the potential for blocking 911 calling and other emergency response services.

Furthermore, any such solution also would need to be forward-looking; it would not be feasible or practical to develop such capabilities for a wide variety of devices running older software and which may no longer even be supported by their manufacturers. This would be true of any form of technical solutions, including “kill switch” software embedded in devices, remote attacks on device OS bootloaders, or pre-installed code that interacts with local beacons.⁴³

Each of these issues needs to be considered in light of the serious risks to public safety presented by contraband phones. Accordingly the Commission must give further consideration and obtain further stakeholder input before mandating actions that would enable a party other than an authenticated owner to fully disable a consumer device.

V. IF CARRIERS ARE REQUIRED TO TERMINATE SERVICE, CERTAIN PROTECTIONS MUST BE INCORPORATED INTO THE RULES

The record demonstrates that the Commission should move forward cautiously when evaluating potential new rules to combat the contraband device problem. Many of the new proposals proffered in the *FNPRM* could adversely impact legitimate consumers. If the Commission is to take additional action, it must ensure that these innocent parties are not adversely impacted.⁴⁴

CIS solutions have a history of falsely identifying contraband devices.⁴⁵ MAS solutions minimize the risks associated with inaccuracies because service is not terminated, but rather is

⁴² CTIA Comments at 7; Verizon Comments at 8.

⁴³ *FNPRM*, 32 FCC Rcd at 2382 ¶ 130 (requesting comment on a system of disabling devices through local beacons that interact with software embedded in the devices).

⁴⁴ T-Mobile Comments at 5-7; AT&T Comments at 2, 5.

⁴⁵ T-Mobile Comments at 6-7; AT&T Comments at 6-9.

merely unavailable within the confines of prisons utilizing MAS. Other CIS solutions require CMRS carriers to terminate service to particular devices. This service termination process is not limited to the confines of the prison and potentially impacts the daily lives of legitimate consumers.⁴⁶

A. SERVICE SHOULD ONLY BE TERMINATED PURSUANT TO A COURT ORDER

As a range of commenters demonstrate, the best way to balance the needs of legitimate consumers and prison officials is to require CMRS carriers to terminate service to alleged contraband devices *only* in response to a court order.⁴⁷ As one commenter notes, “use of a court order process will ensure a high degree of accuracy in the termination process, as any request will be required to meet an evidentiary standard sufficient to ensure that lawful device users have not been erroneously captured.”⁴⁸ The record also demonstrates that a court order will help shield CMRS carriers from liability arising from terminating service in response to incorrect or improper requests.⁴⁹ The optimal solution – one that protects both correctional facilities and citizens outside correctional facilities whose rights might be negatively impacted by a too-lenient standard for termination – would be to require the full rigor of judicial process before service to an alleged contraband device can be terminated.

⁴⁶ AT&T Comments at 6-9.

⁴⁷ T-Mobile Comments at 5-8; AT&T Comments at 2-3; 9-13; CTIA Comments at 5-6; Verizon Comments at 4-8.

⁴⁸ AT&T Comments at 2-3.

⁴⁹ T-Mobile Comments at 7-8; AT&T Comments at 13-14.

B. CMRS CARRIERS MUST BE GRANTED LIABILITY PROTECTION

Commenters express significant concern over potential liability from any rules requiring CMRS carriers to terminate service to devices that are misidentified as contraband.⁵⁰ As T-Mobile explained, carrier contracts and terms of service may not prevent litigation arising from “wrongful” service termination.⁵¹ The Commission therefore should adopt a rule insulating CMRS carriers from liability arising from terminating service to alleged contraband devices.⁵²

C. CMRS CARRIERS MUST BE ENTITLED TO RECOVER THE COSTS ASSOCIATED WITH COMPLIANCE

T-Mobile continues to urge the Commission to expressly authorize CMRS carriers to recoup all costs incurred as a result of a CIS deployment. This would be both in keeping with good policy, and with precedent with regard to 911 services and responding to requests from law enforcement. Cost recovery is not intended for profit, but rather is designed to recover reasonable costs incurred while complying with legally required law enforcement support actions.⁵³

VI. THE RECORD DEMONSTRATES OPPOSITION TO PRIOR NOTIFICATION REQUIREMENTS

The record contains significant opposition to any rules that would require CMRS carriers to provide advance notification to CIS providers of network and frequency changes. Such notification requirements would impede carrier network management flexibility and could delay the deployment of new technologies and services to the detriment of consumers.⁵⁴ Furthermore, it is not practical to provide notifications for many network changes as they are routinely

⁵⁰ T-Mobile Comments at 11-12; CTIA Comments at 9.

⁵¹ T-Mobile Comments at 12.

⁵² *Id.* at 11-12; CTIA Comments at 9.

⁵³ *See* T-Mobile Comments at 10-11.

⁵⁴ T-Mobile Comments at 13-14; CTIA Comments at 7-8; Verizon Comments at 3, 10-11.

implemented in response to real time environmental changes and, in some cases, done without human interaction.⁵⁵

CONCLUSION

T-Mobile respectfully submits that the best course of action for the Commission is to allow recent rule changes supported by a wide range of stakeholders the chance to be fully implemented and assessed. The record indicates such a course of action would go a long way to help resolve the issue of contraband devices in correctional facilities and would probably obviate the need for additional regulations.

Respectfully submitted,

By: /s/ Steve Sharkey

Steve Sharkey
Eric Hagerson

T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004
(202) 654-5900

July 17, 2017

⁵⁵ Cellblox misrepresents that the great majority of network changes, even routine ones, are planned out well in advance (*i.e.*, more than 90 days beforehand) – this is simply not the case. *See* Initial Comments of CellBlox Acquisitions, LLC, GN Docket No. 13-111, at 5-6 (filed June 19, 2017).