February 20, 2018

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: *Ex Parte* Filing in GN Docket No. 13-111, *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*

Dear Ms. Dortch,

The Center for Democracy & Technology (CDT) and the Electronic Frontier Foundation (EFF) write to express concerns regarding the proposals under consideration to stem the use of contraband wireless devices in correctional facilities. We share the interest of the Commission in protecting the welfare of facility administrators, law enforcement authorities, and the general public. However, mandates for hard kill switches and proprietary technology will create new security vulnerabilities, and the lack of judicial review within the kill switch process will violate established protections for due process. With this in mind, CDT and EFF respectfully request that the Commission reconsider the following proposals.

I. Mandate for Hard Kill Switch for Wireless Devices

First, the proposed mandate for a hard kill switch for wireless devices will create new security risks for the general public.[1] The proposal will force service providers and manufacturers to create a vulnerability in all wireless devices to allow providers to permanently disable a device if it is being used illicitly in a correctional facility.[2] But this vulnerability will not exist in a vacuum,

[1] A hard kill switch would permanently disable the phone, whereas a soft kill switch can typically be reversed with the authorization of the device owner. Brad Molen, *The government shouldn't regulate smartphone kill switches*, Engadget, Aug. 8, 2014, https://www.engadget.com/2014/08/18/cellphone-kill-switch/.

[2] *In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336, 2372 ¶ 95 (2017) (FNPRM) ([W]e 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…"). *See also* U.S. Department of Commerce, National Telecommunications and Information Administration, Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions at 33 (Dec. 2010) (NTIA Report), *available at* http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010pdf.

and it will be difficult to secure.[3] As a result, malicious actors may be able to hijack or create their own hard kill signal for their own purposes, regardless of where the phone is being used.[4]

Moreover, the use of a hard kill switch poses greater risks to users in the event of erroneous identification. If a device is misidentified as contraband and subsequently disabled, the owner of the device will be permanently deprived of their device without any warning or explanation. Given how many Americans rely on wireless devices as a primary means of communication, the use of a hard kill switch could preclude access to friends, family, and emergency services.[5] Ultimately, this mandate represents an overly broad and severe remedy that will undermine the security and integrity of wireless devices.

II. Lack of Judicial Review

Furthermore, the hard kill switch proposal lacks necessary safeguards to ensure accuracy and preserve due process rights.[6] The prescribed process would compel commercial mobile radio service (CMRS) licensees to permanently disable contraband devices, pursuant to a qualifying request from a correctional facility official that includes specific identifying information regarding the device and the correctional facility.[7] Under these terms, licensees would be thrust into a role typically reserved for judges. Providers would be charged with evaluating whether requests meet the necessary legal criteria without the procedural structure, experience, or institutional authority of the courts.

To protect fundamental due process rights, the permanent disabling of a contraband device should only occur pursuant to a court order.[8] In contrast with CMRS licensees, the courts are institutionally isolated from political pressure and vested with the responsibility to provide oversight of law enforcement requests. And in this instance, courts provide a necessary form of judicial review before the state deprives an individual of property. Under the current terms of the proposal, the government would be ordering the effective destruction of a wireless device

---

[3] Marc Rogers, *Bricks of Silver: Hacking Smartphone Theft*, Recode, Feb. 18, 2014, https://www.recode.net/2014/2/18/11623586/bricks-of-silver-hacking-smartphone-theft.

[4] *Id.* ("The ability to kill large numbers of phones in an area, or even a country, would be attractive to everyone from mischievous 'black hat' hackers to organized criminals, and even terrorists.").

[5] 95 percent of Americans now own a cellphone of some kind, and 77 percent of U.S. adults own a smartphone--up from a mere 35 percent in 2011. *Mobile Fact Sheet*, Pew Research Center, February 5, 2018, http://www.pewinternet.org/fact-sheet/mobile/.

[6] We also have similar concerns regarding the use of soft kill switches. From a policy perspective, the courts can provide a valuable review of law enforcement actions and potentially reduce the misidentification of contraband devices before service is discontinued.

[7] FNPRM, 32 FCC Rcd at 2372 ¶ 95.

[8] As noted in comments submitted in response to the FNPRM, a court order requirement would be consistent with the standard that the government must meet in similar contexts. *See* Comments of T-Mobile USA, Inc., GN Docket 13-111, at 5-6 (filed June 19, 2017) ("T-Mobile Comments").

by permanently disabling it, subject only to the review of a private actor. But before depriving an individual of their property, the government should allow for some form of due process.[9] Without providing for some form of judicial review, the current proposal under consideration by the Commission would fall far short of the requirements established under the Constitution.[10]

III. Mandate for Proprietary Technology

Finally, in regards to potential technologies that may stem the use of contraband wireless devices, we would caution the Commission against a mandate for proprietary technology. In particular, the FCC appears to be considering a proposal that would disable contraband devices through a beacon system and software embedded in wireless devices.[11] Much like the mandate for a hard kill switch, a mandate for proprietary technology to disable wireless devices would represent a vulnerability that would endanger the integrity and security of these devices. It would represent a singular attack point that could be exploited by malicious actors to disable wireless devices. Additionally, a mandate would stifle the development of new innovative solutions that may effectively address the problem at a lower cost by creating new barriers to entry.

For the above reasons, CDT and EFF urge the FCC to include due process safeguards in its proposals and reconsider mandates for hard kill switches and proprietary technology for wireless devices.

---

[9] Soldal v. Cook Cnty., 506 U.S. 56, 62-63 (1992) ("[O]ur cases unmistakably hold that the [Fourth] Amendment protects property as well as privacy…A 'seizure' of property occurs where there is some meaningful interference with an individual's possessory interests in that property.") (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)); Lavan v. City of Los Angeles, 693 F.3d 1022 (9th Cir. 2012) (finding that the seizure and destruction of property interferes with Fourth Amendment possessory interests and is subject to due process requirements).

[10] While prisoners are entitled to a reduced level of due process protections, the hard kill switch proposal outlined by the FCC may not be limited strictly to phones in correctional facilities due to technological limitations. As a result, the devices of law-abiding consumers outside of the correctional facility may be misidentified as contraband devices and subsequently disabled. *See* Comments of AT&T Services, Inc., GN Docket 13-111, at 5-9 (filed June 19, 2017); T-Mobile Comments at 6-7; Comments of Verizon, GN Docket 13-111, at 12-13 (filed June 19, 2017).

[11] FNPRM, 32 FCC Rcd at 2382 ¶ 130.