RESEARCH REPORT

# Cell Phone Jamming Technology for Contraband Interdiction in Correctional Settings

*John Shaffer*
CONSULTANT

*Bryce Peterson*
CNA CORPORATION

*KiDeuk Kim*
URBAN INSTITUTE

*Rochisha Shukla*
URBAN INSTITUTE

*with Joseph Russo and Megan Kizzort*

*June 2023*

URBAN INSTITUTE · ELEVATE · THE · DEBATE


## ABOUT THE URBAN INSTITUTE

The Urban Institute is a nonprofit research organization that provides data and evidence to help advance upward mobility and equity. We are a trusted source for changemakers who seek to strengthen decisionmaking, create inclusive economic growth, and improve the well-being of families and communities. For more than 50 years, Urban has delivered facts that inspire solutions—and this remains our charge today.

# Contents

# Acknowledgments

This report was funded by award number 2019-UP-BX-K001, awarded by the US Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. We are grateful to them and to all our funders, who make it possible for Urban to advance its mission.

The views expressed are those of the authors and should not be attributed to the Urban Institute, its trustees, or its funders. Funders do not determine research findings or the insights and recommendations of Urban experts. Further information on the Urban Institute's funding principles is available at urban.org/funding principles.

We would like to thank several people for speaking to us about their experiences with contraband cell phone jamming technologies, including Todd Craig, acting assistant director, chief of security technology, Federal Bureau of Prisons (retired); Sue Wilson, assistant commissioner, Corrective Services NSW (retired); Neil Attridge, manager electronic security, New Zealand Department of Corrections; and Bryan Stirling, director, South Carolina Department of Corrections. We would also like to thank David Pitts from Urban Institute for reviewing and providing feedback on this report.

# Cell Phone Jamming Technology for Contraband Interdiction in Correctional Settings

Cell phones have become a ubiquitous part of society, with more than 97 percent of US adults owning one (Pew Research Center 2021). For prison and jail officials, however, they represent a serious and growing concern. In a recent survey of state correctional agencies, Urban found that most respondents consider cell phones a serious problem for a facility's overall security and for the safety of incarcerated people, staff, and members of the public (Kim, Peterson, and Shaffer 2023).

Corrections officials have employed several technological and nontechnological solutions to address contraband cell phones in their institutions (Peterson et al. 2022; Russo et al. 2022). No one strategy appears to be completely effective at combating contraband cell phones. Most strategies are limited in their ability to prevent cell phone use across an entire facility, while others are difficult to implement or prohibitively expensive (see Peterson et al. 2022). Conversely, signal jamming has received broad support among criminal justice practitioners as a potentially effective and straightforward interdiction strategy.[1] Officials can use signal jamming to prevent people from using cell phones throughout their facilities by compromising a phone's ability to receive signals or by modifying received signals to be inaccurate or inoperable. A typical application of cell phone jamming involves overwhelming the phone with a higher-power signal, usually a pure signal or random noise, so the phone can no longer function properly.

Although many corrections officials are interested in implementing signal jamming in their agencies, the Federal Communications Commission currently prohibits the use of this technology in the United States, as guided by the Communications Act of 1934.

---

*"No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government." —Communications Act of 1934, 47 USC § 333*

---

Some federal agencies are exempt from the Communications Act and are allowed to implement jamming solutions by requesting and receiving Special Temporary Authority licensing from the Federal Communications Commission. The Federal Bureau of Prisons is among these agencies. No state or local entities are currently allowed to use signal jamming technology. The selective prohibition against jamming has been a source of tension between federal regulators and corrections officials, and federal lawmakers have made efforts (for instance, through the Cellphone Jamming Reform Act of 2022) to revise the Communications Act and allow state correctional agencies to jam cell phones. Despite corrections officials' interest in jamming and the ongoing discussion around legislative changes, little is known about the use and application of this technology in correctional settings.

To address this knowledge gap, the Urban Institute, along with partner organizations (CNA Corporation, Correctional Leaders Association, and American Correctional Association) and subject-matter experts (John Shaffer and Joe Russo), reviewed current industry practices and interviewed officials with firsthand experience implementing jamming. In summer and fall 2021, we spoke with corrections officials in the United States, New Zealand, and Australia to formulate an understanding of the benefits and challenges of cell phone jamming as a cell phone interdiction strategy.[2] This report is a resource for stakeholders and the public on the mechanics of jamming, its potential effectiveness, and the legal and pragmatic considerations involved in its implementation in correctional settings.

# Basics of Jamming Technology

Cell phones and similar devices use radio frequency (RF) to transmit and receive signals. This makes these devices susceptible to interference, such as through signal jamming. Although the mechanics of jamming technologies are nuanced and complex, there are three basic approaches to RF signal jamming:

- **Brute force jamming** (also known as wide-band jamming or noise jamming), involves transmitting high-power electronic "noise" across multiple frequencies to disrupt all RF communications in an area.
- **Micro-jamming** (also known as narrow-band jamming or surgical jamming), involves transmitting low-power electronic "noise" using the same frequency as the targeted devices in an area.
- **Spoofing** involves installing a local cell tower near the target area to intercept nearby RF signals and return a DoS (Denial of Service) message to the cell phone user.

**Brute force jamming** is the introduction of indiscriminate RF signals transmitted at a power higher than the targeted wireless device(s). The jammer overwhelms the RF spectrum and interferes with wireless signals so they cannot be received or decoded properly at the wireless receiver station. The effective range of the brute force jammer depends on the RF power transmitted by the jammer, distance to the target(s), and environmental factors (e.g., building structures, furniture, vehicles, dense vegetation, inclement weather). The principal application for brute force jamming is for the military to interrupt enemy communications and to disrupt the wireless detonation of roadside improvised explosive devices. The military and authorized federal agencies also deploy brute force jammers for executive-protection missions.

Because brute force jamming effectively interrupts all wireless communications, a significant concern about this technology is "signal bleed," whereby the signals that jam radio frequencies leak outside the intended area (e.g., a prison), interfere with emergency calls, and create serious risks for public safety communications. This is particularly relevant to correctional facilities that are close to other public-access areas. Brute force jamming thus can inadvertently jam emergency calls and other legitimate, private calls made from such areas.

**Micro-jamming** works similarly to brute force jamming but involves a more reactive, targeted, and low-power approach. In most micro-jamming installations, small receiver/transmitter devices are installed in a distributed antenna system (DAS) array in the targeted area. In a correctional environment, these receiver/transmitter devices would typically be installed in the pipe chases between prison cells or along the walls or in the ceilings of open dormitory areas. When a receiver detects a cell phone's RF uplink signal (that is, when a user attempts to initiate or receive a voice call or SMS text message), the micro-jammer instantly reacts by transmitting an RF signal at a slightly higher power on the same frequency to interrupt the downlink communication between the cell phone and the carrier's tower. The system detects the discrete operating frequency, power, and range of the targeted device and terminates the transmission on the same frequency without interfering with other legitimate radio frequencies that may be operating in the environment.

As with brute force jamming, there are concerns that micro-jamming will affect wireless devices being used outside of the targeted area (e.g., the perimeter of a correctional institution). But as we note below, our team learned from conversations with corrections officials that such RF leakage from micro-jamming technologies can be limited to within 12 inches of the intended containment boundary. Thus, there is some promise that micro-jamming can be deployed in correctional facilities without interfering with public wireless services outside the secure perimeter.

The third approach to signal jamming, **spoofing**, involves the installation of a cell tower near the targeted area that will intercept nearby RF signals and return a DOS (denial of service) message to the user. In general, a cell phone connects to the nearest communications tower in its immediate proximity. A local spoofing tower captures all RF signals upon detection before they can reach legitimate carrier towers. In the correctional environment, this would require a tower to be very close to the facility (perhaps within 1,000 to 1,500 feet). Like brute force jamming, a spoofing tower is indiscriminate, and it is difficult to contain its coverage area. The effective range of the spoofing tower depends on the ambient RF power, distance to the target(s), and environmental factors (e.g., building structures, furniture, vehicles, dense vegetation, inclement weather). Currently, as with both other forms of jamming, only authorized federal agencies and the US military can deploy spoofing technology.

# Uses, Efficacy, and Implementation Considerations

Although most correctional agencies in the United States are prohibited from using them, jamming technologies are routinely used by correctional agencies around the world. Early adopters of jamming include New Zealand, which implemented the technology in 2009, and Australia, which started its trial of jammers in 2013.[3] In the United States, the Federal Bureau of Prisons conducted an early test of brute force jamming in February 2010 and a limited field test of micro-jamming technology at the Federal Correctional Institution in Cumberland, Maryland, in January 2018 (NTIA 2018). A subsequent test of micro-jamming was conducted in a South Carolina Department of Corrections facility, with oversight provided by the Federal Bureau of Prisons and its legal authority (DOJ 2019). Drawing from our conversations with the correctional officials from Australia, the Bureau of Prisons, New Zealand, and the South Carolina Department of Corrections who have hands-on experience testing and using jamming technologies, we have identified several key considerations about the potential efficacy and implementation challenges associated with this technology.

## Overall Efficacy of Jamming

Corrections leaders reported that signal jamming technology has been effective in shutting down access to phone signals entirely in implementation zones. Additionally, compared with other commonly used solutions in the United States that have inherent delays before shutting down signals (e.g., managed access systems, or MASs), jamming technologies shut down signals almost instantaneously.

The systems are not foolproof, however, and require frequent monitoring, maintenance, and calibration to remain effective. There can be gaps in jamming coverage because of building structure interference and other environmental factors. Jammers also suffer from the same challenges as other interdiction solutions. For example, people inside or outside a facility could destroy the jamming sensors to render them inoperable. There can also be ways to circumvent the technology, such as finding a "dead spot" in the facility (an area where jamming does not work and people can use cell phones). Furthermore, many jamming solutions are calibrated to only work on an RF from cell towers and do not block Wi-Fi or prevent the use of satellite phones (though they technically could jam Wi-Fi and satellite frequencies if legally authorized). Thus, if incarcerated people can access Wi-Fi, such as by working with an accomplice to set up a hot spot outside the facility, they would be able to defeat the jammer.

Though jamming systems can terminate voice communication, data, and SMS text messaging services from illicit cell phones, the devices' other features are still functional. In other words, cell phones are still capable of taking videos and photographs, creating voice recordings, and being used as word processors. Videos, pictures, documents, and other data from cell phones can then be smuggled out of the facility on the cell phone itself or on removable storage devices, such as SD cards. Because this information is often sensitive and because of privacy and security concerns, correctional staff view this as dangerous and detrimental to facility security. Similarly, people can use these tools to smuggle harmful materials, such as child pornography, into facilities for distribution.[4]

## Containment Accuracy

As we discuss above, a potential concern about jamming is signal bleed. The corrections officials we spoke with reported that micro-jamming technologies are accurate and minimize signal bleed to the containment area. In some cases, this is limited to within 12 inches of the jamming zone. Thus, a properly calibrated micro-jamming system will likely not disrupt cell phones outside a facility. But achieving proper calibration requires constant monitoring by agency staff and coordination with the jamming technology vendor to ensure there is no signal bleed and to minimize "dead spots."

In addition, micro-jamming does not work well outdoors because the sensors must be placed approximately 10 to 20 feet apart to be effective. Most agencies that have piloted or are currently using signal jamming technologies only use them in indoor spaces. For example, they will jam RF signals within housing units, dining areas, workshops, and so on, but not in the outdoor areas of the facility available to incarcerated residents (e.g., outdoor recreational spaces and pathways between buildings). The decision

not to jam in outdoor spaces owes primarily to the issues, and associated costs, around containing signal bleed. Thus, there are notable deficiencies in jamming in facilities that have large amounts of outdoor space.

## No Option to Whitelist

Managed access systems, an interdiction solution used in US prisons as a legal alternative to signal jamming, provide the option of whitelisting certain phone numbers. This means specific authorized cell phones are allowed to be used within implementation zones, and the MAS does not interfere with those phones' signals. Conversely, signal jamming technologies do not have this option and jam all signals within an intended area. Correctional staff and other authorized users cannot use cell phones within implementation zones and must rely on landlines and radios to communicate within the facility. This can be a problem for agencies that provide agency cell phones to their staff or that otherwise authorize staff to use cell phones inside correctional facilities.

## Long-Term Health Effects of Prolonged Exposure to RF Energy

Another concern around the use of jamming technologies is their potential impact on health. There are numerous studies on the health impacts of RF waves people are commonly exposed to, such as those from radio, television, and wireless telephony (Valberg et al. 2007). Overall, there is little support for the notion that these technologies have adverse health effects, such as brain cancer, tumors, or worsened reproductive potential (Merhi 2012; Repacholi et al. 2012).

Jammers, however, are unique in that most operate by constantly emitting RF energy that jams cell phone signals. Corrections staff could be exposed to this RF energy for tens of thousands of hours over their careers, while incarcerated residents would be exposed constantly during their stays in facilities equipped with jammers. No studies have examined the long-term health effects associated with prolonged exposure to this energy. Some jammers only emit RF energy when they detect active signals from cell phones, though these would likely still result in significant exposure to such energy. Correctional administrators and researchers should consider these concerns as they push for or move forward with implementing jamming technologies.

## Challenges to Rehabilitation Efforts

Some correctional officials using jamming technologies are considering moving away from them because they can interfere with electronic tablets agencies are providing to incarcerated people. Many prison and jail officials have introduced or are planning to introduce these tablets, which provide incarcerated residents email communication, video visitation, educational and vocational training, and therapeutic program content. Though officials could exclude the frequencies on which these tablets operate from jamming systems, there is still some concern that jammers would disrupt the wireless connections needed for these tablets and thus impede agencies' rehabilitative efforts. Because of this, officials in New Zealand have begun retiring jamming in their prisons and explored alternative interdiction solutions, such as MASs, which allow them to whitelist tablets authorized for their incarcerated residents more easily.

## Implementation and Maintenance Costs

The initial setup costs and ongoing costs are among the biggest limitations to jamming. The technology is expensive to purchase, with estimates ranging from $1.5 to $2.5 million per facility, and ongoing maintenance costs can make them substantially more expensive (see Peterson et al. 2022). This is comparable to other whole-facility interdiction solutions, such as MASs.

The regular maintenance jamming requires is extensive. Correctional officials who have used the technology noted that, to keep up with advances in network technologies (such as upgrades from 3G to 4G to 5G services and other evolutions in cellular technologies), jammers need to be consistently monitored, calibrated, and upgraded. For older systems, such upgrades can only be done by replacing units, which is equivalent to installing a completely new system. Newer systems are designed to allow remote firmware/software upgrades, but these can also require significant investment of staff resources and money. Additionally, windows around the perimeter of an implementation area (e.g., the housing units in a prison) may need to be "shielded" to make the jamming technology more efficient. This involves placing a reflective film on windows to contain the RF energy within the implementation area. This film is expensive and adds to the initial implementation costs. The film is also subject to damage and sabotage (it can be peeled off windows) after it is installed.

# Conclusion

State and local correctional agencies in the United States are currently prohibited from using jamming technologies under the Communications Act of 1934. Many officials from these agencies and other corrections stakeholders have spent years advocating for changes to this law. People pushing for this change believe strongly that signal jamming would equip prison and jail administrators with a reliable and effective tool for combating contraband cell phones. If changes are made to the Communications Act to permit the use of jamming, corrections agencies deciding whether to use the technology will need to consider several factors around its uses, efficacy, and implementation. In this report, we have drawn from the experiences of correctional administrators in the United States and abroad who have piloted or used jamming to detail many of these considerations.

When properly deployed and calibrated, jamming is effective at preventing the use of cell phones to make calls, send text messages, and use data-based services. Likewise, most agencies have been successful at limiting "signal bleed" by containing the jamming cellular signals to the implementation areas in their facilities (e.g., the housing units or other indoor spaces where the technology has been installed).

Despite the promise of jamming, this technology has several potential shortcomings. It does not disable any of a contraband cell phone's other features, such as video and word processing, which can be used by incarcerated people to capture and share sensitive or compromising information. In addition, most agencies would likely only jam cell phones inside facilities' housing units or other indoor spaces because of the challenges associated with jamming signals outside. This limits the efficacy of jammers in preventing illicit communication, particularly in facilities with large recreation yards, farms, or other outdoor areas.

Jamming technologies also have limitations that may make them less desirable to correctional officials than other interdiction strategies, such as MASs. For instance, jammers do not allow officials to "whitelist" cell phones or other wireless devices that rely on mobile networks. This can pose problems to agencies that assign agency cell phones or allow staff to use personal devices. It could also prevent 911 calls and could interfere with tablets or other devices provided to incarcerated residents for treatment and service delivery. In addition, jammers merely prevent people from using their phones to make calls or send text messages and do not capture cell phone transmissions or any cell phone data.

Conversely, with MASs and other detection technologies, correctional agencies can detect or intercept calls, which yields intelligence about the number of illicit phones in a facility and facilitates their confiscation and removal. With MASs, captured transmissions can also generate evidence for

court orders that officials can use to force carriers to permanently disable phones' voice, text, and data-transmission capabilities or deauthorize SIM cards (Grommon et al. 2016). Of course, each alternative interdiction technology comes with unique implementation challenges. For example, MASs are expensive to install, difficult to maintain, and can be limited by the time it takes them to detect and terminate illicit transmissions (California Council on Science and Technology 2012; Peterson et al. 2022).

Finally, it is critical to note that jamming technologies are technically difficult and expensive to implement and maintain. They require regular monitoring, calibration, and updates to keep pace with ever-improving cell phone and network technology. Although they are not legally available to most US correctional agencies, jammers would likely cost at least as much as other permissible technologies, such as MASs or detection/location systems (see Peterson et al. 2022 for descriptions and cost estimates of various contraband interdiction technologies). Agencies would likewise need substantial technical expertise, capacity, and personnel to effectively implement jamming technology.

In short, although jamming holds potential for preventing the communications capabilities of contraband cell phones in prisons and jails, jamming technology is not a panacea for all the challenges cell phones pose to the safety and security of correctional institutions and their staff and residents. Agencies pushing for changes to federal law that would allow them to install jammers in their facilities should consider these shortcomings and continue exploring other legally permissible solutions. To that end, Urban has compiled several resources outlining technological and nontechnological strategies agencies should consider when developing comprehensive approaches to contraband cell phone interdiction (see Peterson et al. 2022 and Russo et al. 2022).

# Notes

[1] Meg Kinnard, "Prosecutors to Congress: Let state prisons jam cellphones," AP News, January 25, 2023, https://apnews.com/article/drug-crimes-alan-wilson-kevin-mccarthy-columbia-south-carolina-c617c572b7252ad60545afe078d6c0d4.

[2] Between April and June 2021, we had informal conversations via Zoom with two officials in the United States, one in New Zealand, and one in Australia. Both New Zealand and Australia were early adopters of microjamming in correctional settings, and the United States has conducted two tests to evaluate its usability. In this report, findings which cite the perspectives and experiences of corrections officials are drawn from these conversations.

[3] Allie Coyne, "NSW kicks off prison mobile jamming trial," IT News, September 14, 2013, https://www.itnews.com.au/news/nsw-kicks-off-prison-mobile-jamming-trial-358000.

[4] Associated Press, "Inmate admits possessing child porn inside federal prison," AP News, April 11, 2018, https://apnews.com/article/3d8a224869bb4637827a675de329e7ed.

# References


California Council on Science and Technology. 2012. *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons.* Sacramento: California Council on Science and Technology.

DOJ (Department of Justice). 2019. *Bureau of Prisons Tests Micro-Jamming Technology in South Carolina Prison to Prevent Contraband Cell Phones.* Washington, DC: DOJ.

Grommon, Eric, Jeremy G. Carter, Fred Frantz, and Phil Harris. 2015. *A Case Study of Mississippi State Penitentiary's Managed Access Technology*. Rome, NY: Engility Corporation.

Kim, KiDeuk, Bryce Peterson, and John Shaffer. 2023. *Technical Assistance Opportunities Around Contraband Cellphone Interdiction: A Bureau of Justice Assistance-Funded Initiative [Webinar].* Hagerstown, MD: American Jail Association.

Merhi, Zaher. 2012. "Challenging Cell Phone Impact on Reproduction: A Review." *Journal of Assisted Reproduction and Genetics* 29 (4): 293–97.

NTIA (National Telecommunications and Information Administration). 2018. *Emission Measurements of a Contraband Wireless Device Jammer at a Federal Prison.* Washington, DC: NTIA.

Pew Research Center. 2021. *Mobile Fact Sheet*. Washington, DC: Pew Research Center.

Peterson, Bryce, KiDeuk Kim, Rochisha Shukla, and Megan Kizzort. 2022. *Interdiction Technologies and Strategies for Contraband Cell Phones.* Washington, DC: Urban Institute.

Repacholi, Michael H., Alexander Lerchl, Martin Röösli, Zenon Sienkiewicz, Anssi Auvinen, Juergen Breckenkamp, and Guglielmo d'Inzeo, et al. 2012. "Ystematic Review of Wireless Phone Use and Brain Cancer and Other Head Tumors." *Bioelectromagnetics* 33 (3): 187–206.

Russo, Joe, Rochisha Shukla, Bryce Peterson, and KiDeuk Kim. 2022. *Nontechnological Challenges in Managing Contraband Cell Phones: A Look at Organizational Culture and Staffing in Correctional Facilities.* Washington, DC: Urban Institute.

Valberg, Peter A., T. Emilie Van Deventer, and Michael H. Repacholi. 2007. "Workgroup Report: Base Stations and Wireless Networks—Radiofrequency (RF) Exposures and Health Consequences." *Environmental Health Perspectives* 115 (3): 416–24.

# About the Authors

**John Shaffer** is an independent consultant and nationally recognized expert on corrections technology. He is currently the Institutional Corrections Program Manager for the Criminal Justice Technology Evaluation Consortium and has authored and coauthored numerous publications under NIJ/BJA grant-funded initiatives, including: Mitigating Contraband Via the Mail; Countering Threats to Correctional Institution Security; Test and Evaluation of Hand-Held Cell Phone Detection Devices; Fostering Innovation in Community and Institutional Corrections – Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector; and Cell Phone Forensics in a Correctional Setting. Shaffer retired from his position as executive deputy secretary for the Pennsylvania Department of Corrections after a 31-year career. He also served as a counselor, human resource analyst, business manager, deputy superintendent, and deputy secretary for administration. He was the interim warden at the Allegheny County Jail in Pittsburgh for nearly a year in 1996. He also served for many years on the National Law Enforcement and Corrections Technology Committee—Northeast Regional Advisory Committee. He was an active member of the NIJ Sensors, Surveillance and Biometrics Technology Work Group, the American Correctional Association, and the PA Prison Wardens Association. Shaffer holds a BA in sociology from Westminster College, and a master of public administration and a PhD in public administration from the University of Pittsburgh.

**Bryce Peterson** is a research scientist in CNA's Center for Justice Research and Innovation. His research focuses on correctional policy, children of justice-involved parents, and technological interventions in criminal justice settings. He received his PhD in criminal justice from the John Jay College/The Graduate Center, City University of New York.

**KiDeuk Kim** is a senior fellow in the Justice Policy Center at the Urban Institute, where he leads multidisciplinary research teams to examine issues related to criminal justice interventions and policies. He has extensive research experience and national expertise in data-driven decisionmaking in criminal justice.

**Rochisha Shukla** is a senior research associate in the Justice Policy Center, where her research portfolio centers around institutional safety, correctional technology, community corrections, and reentry. Before joining Urban, Shukla completed her master's degree in criminology and criminal justice from the University of Maryland, College Park.

## Statement of Independence

The Urban Institute strives to meet the highest standards of integrity and quality in its research and analyses and in the evidence-based policy recommendations offered by its researchers and experts. We believe that operating consistent with the values of independence, rigor, and transparency is essential to maintaining those standards. As an organization, the Urban Institute does not take positions on issues, but it does empower and support its experts in sharing their own evidence-based views and policy recommendations that have been shaped by scholarship. Funders do not determine our research findings or the insights and recommendations of our experts. Urban scholars and experts are expected to be objective and follow the evidence wherever it may lead.


500 L'Enfant Plaza SW
Washington, DC 20024

*www.urban.org*