Criminal Justice Testing and Evaluation Consortium
A Program of the National Institute of Justice

Detecting and Managing
Cell Phone Contraband

An overview of technologies for managing contraband cell phone presence and use in correctional facilities

This technology brief is part of a series of documents that focuses on contraband in corrections. This document specifically focuses on detection and management of cell phones. Additional documents provide information on contraband, including types of associated technologies and products used to detect contraband on people, in vehicles, and in an environment. The goal of this series is to offer foundational insights from use cases, highlight challenges of contraband detection, compare illustrative products, and discuss the future of contraband detection and management.

Key Takeaways

- Continuous advances in cell phone technology make disruption and deterrence efforts a challenge, yet products are emerging to help correctional facilities detect cellular devices and componentry.
- Cell phone detection technologies may be limited by their range or the need for cell phones to be powered on and in use at the time of detection. Among devices used by correctional facilities, technologies such as radiofrequency detection (RFD) that can locate a cell phone signal or recognize the presence of cellular components being trafficked at multiple locations within a facility demonstrate the greatest promise for successful interdiction.
- There are technologies emerging such as micro-jamming and managed access systems that disrupt and disable cell phone signals, but they have disadvantages related to potential interference with federal policies, high cost, and the fact that phones may still function (e.g., using Wi-Fi for other communication methods).

Contraband is a significant problem in correctional facilities throughout the United States because it can pose a threat to the safety of individuals who live and work inside correctional facilities, as well as for the general public. Detecting and managing contraband in facilities is an important step to minimize risks to all stakeholders involved. Of the various forms of contraband, cell phone contraband is one of the fastest growing and most significant challenges for many correctional facilities.[1] This brief summarizes solutions for detecting and managing cell phone contraband, lays out the associated benefits and limitations of its use in correctional facilities, provides types of detection technologies and associated products, and discusses potential future needs and considerations for managing cell phone contraband in facilities across the United States.[2]

Contraband Detection Solutions for Correctional Facilities

This document explores cell phone contraband detection technologies. Additional documents in this series address specific contraband topics.

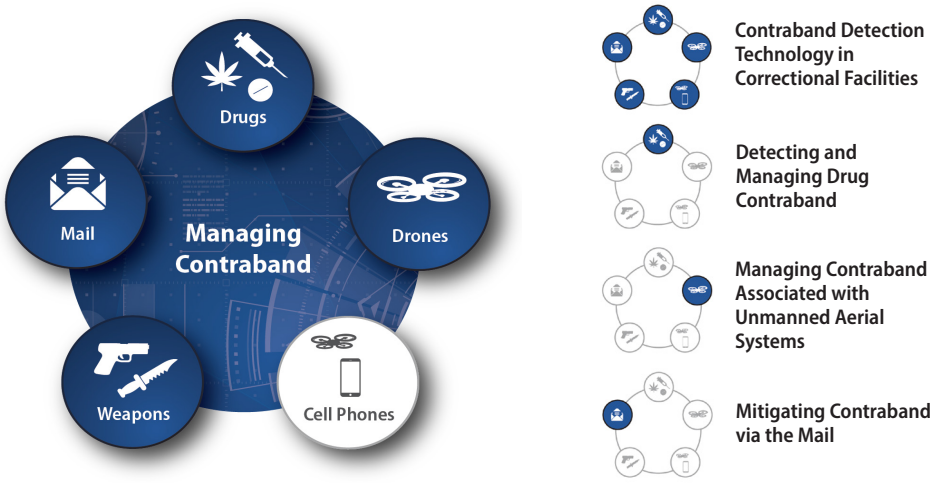


Figure 1: The successful management of cell phone contraband requires trade-offs related to performance, price, and operational issues.

1. U.S. Department of Justice, Office of the Inspector General. (2016, June). *Review of the Federal Bureau of Prisons' contraband interdiction efforts*. Retrieved from https://www.oversight.gov/sites/default/files/oig-reports/e1605.pdf
2. Products referenced within this document are used for illustrative purposes and do not represent NIJ's or CJTEC's recommendation, endorsement, or validation of product claims.



Cell phones are a problem for correctional facilities.

Over the past decade, contraband cell phones have become one of the fastest growing problems facing correctional facilities, reflecting the general rise in cell phone use in society. Widespread presence of cell phones in correctional facilities can be estimated from confiscation data: for example, in 2017,[3]

- South Carolina prison officers found and confiscated one phone for every three inmates;
- Oklahoma prison officers found one phone for every six inmates; and
- Mississippi prisons seized 1,800 cell phones—approximately one phone for every 10 inmates.[4]

Communication via cell phone is commonplace in everyday life, which makes the devices all the more desirable when freedom to communicate is restricted. Beyond traditional mail, inmates are allowed to use monitored communication for conversations with outsiders via banks of three to four landline phones that are shared by groups of inmates, with conversations limited to 5 to 15 minutes. Some prisons have begun using tablets for video chats on a limited basis, but video and landline calls are not without a fee: a brief phone call can cost up to $10.[5] Contraband cell phones provide an avenue for unlimited, unmonitored, and comparatively low-cost communication, including internet access to social media, that is highly attractive to inmates and thus increases the demand for cell phones within prison walls.

Cell phone use by inmates is a significant concern because they can be used to contact accomplices both inside and outside the facility for nefarious purposes, including to:

- Orchestrate escape attempts;
- Manage criminal enterprises, including running scams, distributing drugs, and extorting money;
- Intimidate or arrange for the murder of victims, witnesses, or public safety officers;
- Use as currency to barter with other inmates; and
- Record and post pictures/video that compromise facility safety and undermine prison management.

As contraband, cell phones have dual functionality: inmates may transmit messages/information via cellular service without requiring physical contact, or they may use the phones as audio/visual recording devices that can later be transmitted via cellular service, Wi-Fi, Bluetooth, or physical exchange. A phone's unique use as a data storage device can be powerful and could serve as a way to share information about facility layout or conditions, thus compromising security measures. The ability to share messages or instructions stored either within the phone's memory or on a Subscriber Identity/Identification Module (SIM) card may be relayed to others if a phone or its components can be passed along.

Despite restrictions, including regulations,[6] cell phone contraband finds entry points into correctional facilities: phones (or their components) may enter via several routes:

- Smuggled in within objects or body cavities
- Brought by visitors and accomplices
- Carried into the facility by unscrupulous correctional employees
- Thrown over or dropped by drone over the perimeter fence
- Delivered via shipments of consumables

For correctional staff, dealing in cell phone contraband exchanges may be tempting, unlike drugs or weapons (which may be illegal or highly suspicious to possess), staff bringing an additional phone into the facility with the intent to leave it with an inmate is difficult to detect, since owning multiple cellphones is neither unusual nor against the law.

3. Hynes, M., & Jordan, N. (2019, July 16). *How to cure prisons' contraband mobile phone epidemic*. Security. Retrieved from https://www.securitymagazine.com/articles/90543-how-to-cure-prisons-contraband-mobile-phone-epidemic
4. Riley, M. (2017, July 30). *Southern prisons have a cellphone smuggling problem*. NBC News. Retrieved from https://www.nbcnews.com/news/corrections/southern-prisons-have-smuggled-cellphone-problem-n790251
5. Natalie. (2019). *Can you have phones in prison?* Prison Insight. Retrieved from https://prisoninsight.com/can-you-have-phones-in-prison/
6. The 2010 Contraband Cellphone Act criminalized possession or introduction of a mobile device or SIM card as dangerous contraband for a federal prison; federal inmates convicted of possessing contraband in prison receive consecutive (or additional) prison time after their original sentence is completed.

Detection strategies are based on how a cell phone is built or functions.

Cell phones have historically consisted of three basic parts: the phone shell (containing electronics, keypad, microphone, speaker, etc.), an associated charger, and the SIM card. Both the phone and SIM card components are necessary for the cell phone to operate as a cellular-based communications device or to record or play data needed for communication. Most phones lacking a SIM card have limited utility; however, SIM cards may store and relay data independent of the phone. Phones consist mostly of plastic with some metal parts for the electronics, whereas SIM cards contain silicon integrated circuits that are manufactured from semiconductors, which are sheathed in plastic. Cell phones are becoming smaller and more powerful with increasing functionality as the technology continues to develop. As technology has advanced, both phones and SIM cards have decreased in size: most common-use phones measure 15 cm,[7] but mini phones may be as small as 5 cm,[8] as demonstrated in **Figure 2**. Furthermore, as depicted in **Figure 3**, standard SIM cards are generally 15x25 mm, but a nano-SIM card may run as small as 12x8 mm.[9]



Figure 2: A mini cell phone approximately 5 cm in length is easily hidden, can transmit phone calls, and is Bluetooth capable.

Along with cell phones, associated chargers are commonly smuggled into correctional facilities; however, many prisons do not have electrical outlets in the cell block. Unlike in a home where outlets are readily accessible, inmates may need to devise ingenious ways to hook up chargers or manipulate existing 110-v power sources found in cells, commissaries, or recreational areas. Inmates use spliced wires taken from electrical devices, such as lamps and computer mice, to steal power from light switches, televisions, and even CPAP machines used for the treatment of sleep apnea. Correctional staff may also assist in charging an inmate's cell phone as a favor or for a fee.

The first step in limiting the number of cell phones and components in a correctional facility is to keep them from entering. Routine screening and restrictions at the point of entry currently occur using screening measures for visitors, staff, and personal items; nonetheless, cell phone contraband still finds its way into facilities.[10] The following strategies provide insight to techniques that can be used independently or as a multilayered approach to cell phone interdiction efforts:

- Point-of-entry detection using scanning technologies
- Environmental detection solutions that enable discovery of cell phones inside the correctional grounds
- Cellular-disabling technologies that eliminate/block the transmission of cellular signals



Figure 3: A nano-SIM card is smaller than a coin and easy to conceal and smuggle into and out of a correctional facility.

7. For example, Redmi Note 7 Pro, Apple iPhone XS, and OnePlus 7. Prawesh Lama, P. (2019, August 26). *Stomach this: Tihar inmates caught swallowing mini phones to beat ban*. Hindustan Times. Retrieved from https://www.hindustantimes.com/delhi-news/stomach-this-tihar-inmates-caught-swallowing-mini-phones-to-beat-ban/story-NsSIV1372rBN70FzN9y9IM.html
8. Antony, T. (2019, November 12). More devices to prevent phones and drug smuggling into jails. *New Indian Express*. Retrieved from https://www.newindianexpress.com/states/kerala/2019/nov/12/more-devices-to-prevent-phones-and-drug-smuggling-into-jails-2060377.html. This cell phone is so small that it may defeat netting designed to catch contraband thrown over the fence into correctional facilities.
9. No author. (2017, February 24). *Your smartphone SIM Type: standard SIM, micro SIM or nano SIM*. Retrieved from https://kenstechtips.com/index.php/smartphone-type-standard-sim-micro-sim-or-nano-sim
10. Cell phones may also be smuggled into a correctional facility via drone delivery, which is discussed in a Capsule within this contraband series.

Managing cell phone contraband requires a multilayered system of defense.

The demand for cell phones is a constant threat within the prison system; contraband devices facilitate a myriad of illicit and criminal activities within prison walls. Employing a multilayered system of defense that harnesses technology at the point of entry and within the facility itself can inhibit inmates' capability to use devices while incarcerated and can provide a highly effective interdiction strategy. Figure 4 provides an overview of a multilayered system of defense to reduce cell phone contraband within correctional facilities. By adopting this approach, prisons can control the trafficking and use of cell phones by reinforcing access points with physical searching, screening of both people and parcels, and technology to disrupt cell signals.

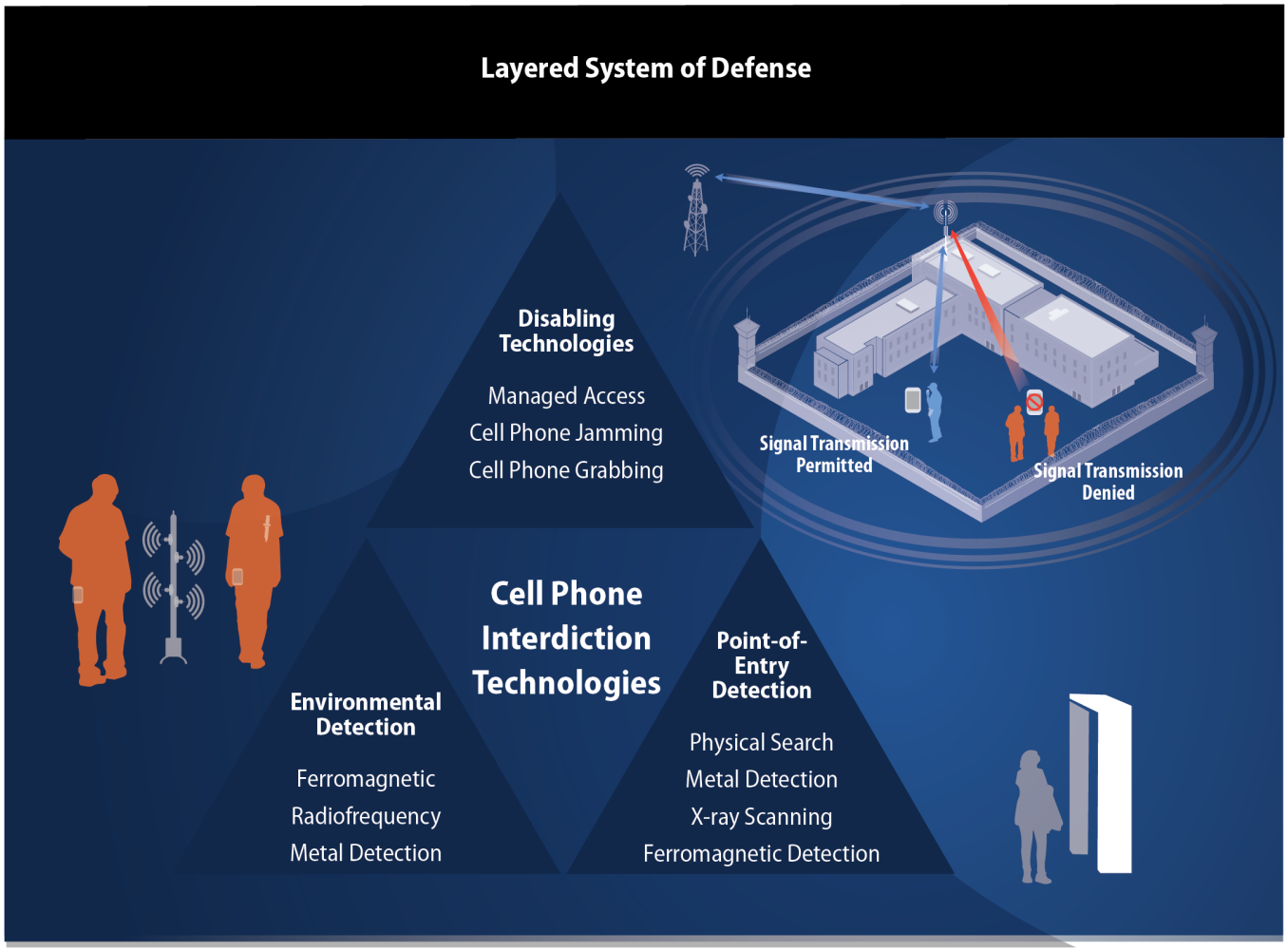


Figure 4: Adopting a multilayered approach enables correctional facilities to control cell phone introduction and use by employing multiple effective strategies.

Detection Technologies

On-site detection devices can provide screening for cell phones and SIM cards at a relatively close range. These devices may identify contraband cell phones (or SIM cards) that could then be confiscated. In Figure 5, the technologies listed are specifically used to detect cell phones and associated componentry contraband.

Comparison of On-Site Cell Phone Detection Devices

Detection Technology	Cost	Detect Cell Phone		Detect SIM Card Separate from Phone	Directional Accuracy	Format & Range (if available)
		ON mode	OFF mode			
Transmission X-ray	$$$$	✓	✓	✓	●	Stationary, Drive-through
Multi-frequency Metal Detection	$-$$	✓*	✓*		◒	Handheld, Stationary
Ferromagnetic	$	✓	✓		○	Handheld, Stationary; Immediate area (0-7")
Radiofrequency	$	✓			●	Handheld; Within a room (70-125 ft)

*Multi-frequency metal detection can detect cell phones in on and off mode, if not obscured in a body cavity.

$ Under $10K
$$ $10K-$25K
$$$ $25K-$100K
$$$$ $100K+

● Excellent
◒ Medium
○ Poor

Figure 5: Cell phone detection technologies have varying costs, ranges, and capabilities that can affect interdiction strategies.

Point-of-Entry Detection

Effectively intercepting illicit cell phone contraband at the point of entry requires physical searching of people and items by vigilant staff and the adoption of supportive technologies to augment their capabilities. As highlighted in the associated contraband briefs within this series,[11] technologies such as X-ray devices provide the capability to identify and locate concealed items on a person or item before entering a correctional facility. Transmission X-ray technologies emit a penetrating form of high-energy electromagnetic radiation that passes through an individual to create an image that can be used to detect cellular device contraband (metallic and nonmetallic) on a person, within a body cavity, through body armor, or inside packages. These systems are typically stationary and used at the points of entry. Figure 6 illustrates a transmission X-ray device commonly used in correctional facilities.

11. Contraband Detection Technology in Correctional Facilities; Detecting and Managing Drug Contraband

Transmission X-ray devices provide the added benefit of being able to locate contraband hidden within body cavities or cleverly integrated into personal items, such as shoes, books, and toiletries. However, X-ray technology is a relatively expensive option and may be cost prohibitive as each body-scanning device can cost up to $250,000. Because cell phones and their associated chargers are composed of ferrous metal components, this type of contraband is also effectively discovered using metal detection and ferromagnetic detection (FMD) systems. The benefit of using metal detection and FMD is their high efficacy in determining the presence of cell phones at a lower cost than X-ray scanning instruments. However, unlike X-ray technology, detecting the presence of metals using metal detectors or FMD systems does not pinpoint the exact location of the contraband; thus, correctional staff have to conduct an additional physical search step.



Image courtesy of Smiths Detection.

Figure 6: Smiths Detection's B-SCAN is a transmission X-ray device that can detect contraband concealed in or on the body.

Environmental Detection Solutions

The use of technologies to detect contraband at the point of entry is essential; however, even when these systems are employed, inmates, staff, and visitors can find ways to overcome these barriers. It is not uncommon for cell phones to be thrown over fences and walls, dropped by drone, hidden within shipments, and smuggled in by corrupt correctional staff and work release inmates. FMD systems and metal detectors have the unique capability of being portable as the devices come in handheld and lightweight form factors that can be employed anywhere within a correctional facility. Because cell phones are inevitably making their way inside prison facilities, employing technologies that can be used to search cellblocks, recreation areas, and commissaries provides significant value. Furthermore, technologies such as RFD devices, which detect cell phone signal transmissions, enable prison staff to discover if cell phones are being used, prompting further investigation.

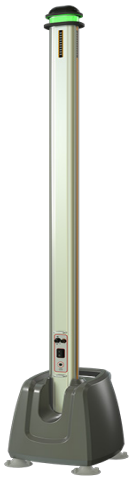


Image courtesy of Metrasens.

Figure 7: Cellsense Plus, offered by Metrasens, features FMDs to detect cell phones among other contraband.

FMD systems, such as the one depicted in **Figure 7**, are primarily handheld or walk-through devices. These devices search for the internal components of a cell phone that contain ferromagnetic materials. Ferromagnetism occurs when materials form permanent magnets or are attracted to magnets. FMD systems use passive sensors that detect a local disturbance in Earth's magnetic field, which is created when ferrous metals pass near the detection area.[12] Common ferromagnetic elements include iron, nickel, and cobalt, which are elements found in most electronics. This technology can passively detect ferrous metals as people and objects move by, allowing more detection in less time and fewer unnecessary close encounters between staff and inmates.[13] FMD systems are lightweight (<20 lbs) and are designed to be portable, enabling correctional staff to locate cell phones and ferrous contraband concealed on a person or in body cavities at various locations throughout the prison. However, FMD systems have a limited range and are best suited for personal searches, as interference from ferromagnetic items within the environment can lead to false positives.

12. Viscardi, J. (2018). Add ferromagnetic detection for better building security. *Buildings*. Retrieved from https://www.buildings.com/articles/27817/add-ferromagnetic-detection-better-building-security
13. Hynes, M., & Jordan, N. (2019). *How to cure prisons' contraband mobile phone epidemic*. Security Magazine. Retrieved from https://www.securitymagazine.com/articles/0543-how-to-cure-prisons-contraband-mobile-phone-epidemic

RFD devices, as demonstrated in **Figure 8**, are typically handheld units that detect radio waves emitted from telecommunication devices. Radio waves are a type of electromagnetic radiation, generated by a transmitter and identified by a receiver. RFD may detect cellular devices on a person or in the environment through handheld devices; however, RFD is only effective when the phone is actively making a call. RFD devices are not able to discover a cell phone in the off position, nor is it able to identify a SIM card by itself.



Image courtesy of Berkeley Varitronics Systems.

Figure 8: RFD detection: Wolfhound-PRO® Cell Phone Detector can detect cell phones in standby mode or while transmitting up to 150 feet away indoors.

Metal detection is the most common type of contraband detection technology found in correctional facilities. These devices can be handheld, as seen in **Figure 9**, providing a useful tool for detecting cell phones inside the facility grounds. These devices can also identify objects containing metal on a person via walk-through or stationary devices but may miss metal (including phones and SIM cards) hidden in body cavities. This type of technology is effective and is the least expensive of the portable devices; however, the devices are limited to a short operating range of several inches, which necessitates a time-consuming manual search of each individual inmate. This process is not as efficient when compared to technologies with a larger detection range, such as FMD systems. Furthermore, metal detection does not distinguish cell phones from other metallic materials, which may often lead to false-positive signals from low-priority objects, such as buttons and hair clips.

A 2016 field assessment of newer cell phone technologies found that corrections officers preferred RFD devices compared to FMD systems. RFD was accurate 100% of the time with no false positives over a wide range (125 ft), whereas FMD produced false positives at a rate of 38% (authorized electronics) to 76% (non-electronics), which frustrated corrections officers.[14] Neither technology offers a perfect solution: RFD devices are limited in that they can only locate a cell phone when it is actively placing a call. This trade-off was worth it to officers given its accuracy (no false positives) and wide range of detection.



Image courtesy of Garrett.

Figure 9: Garrett's Super Scanner V is a handheld metal detector that can locate metal objects hidden underneath clothing.

Environmental detection solutions are advantageous in that they allow for detection of, and thereby the confiscation of, physical devices. Combined with point-of-entry detection systems, such as X-ray and walk-through metal detection systems, environmental detection solutions can drastically reduce the amount of cell phone contraband in a prison. However, the current number of cell phones being discovered and confiscated among inmates suggests that a more robust, multilayered solution is needed, which may necessitate the use of disabling technologies.

14. Russo, J. (2016, April). *Evaluating the performance of hand-held cellphone detectors in a prison setting*. Retrieved from https://www.ojp.gov/pdffiles1/nij/249800.pdf

Disabling Technologies

While detection devices are used to identify cell phones, disabling technologies seek to disrupt their communication functionality (**Figure 10**). If cell phones are rendered inoperable, their desirability as contraband decreases considerably. The primary advantage of these solutions is that they function in the background and, at least theoretically, should not create additional work for corrections officers. There are three main strategies for disabling contraband cell phones:

- **Managed access systems** allow authorized calls (and 9-1-1 calls) to pass through but reject unauthorized calls, such as those placed by or made to inmates. This type of system acts like a cellular base station that picks up and manages all calls made within the prison, and it has shown promise at correctional facilities where it has been trialed. At a correctional facility in Parchman, Mississippi, this technology stopped over 200,000 illegal calls made by/to inmates over a 1-month period.[15]
- **Cell phone grabbing** is permanently installed at a correctional facility. The assessment geo-locates the signal of a contraband device within the facility. Transactional data captured from the contraband cell phone can be used as the basis for a seizure warrant to disable service to the device, subject to correctional staff obtaining a court order from the governing jurisdiction. The Federal Communications Commission has initiated legislation to make shutting off service to a contraband device an administrative request to wireless carriers, rather than requiring a court order. However, a pilot study at a correctional facility in Scotland demonstrated cell phone grabbing technology requires further refinement as it took very little time for inmates to discover their phones were being blocked, detect vulnerabilities, and overcome the phone blocking system with innovative countermeasures.[16]
- **Micro-jamming technology** blocks mobile reception by using a device to transmit a signal on the same frequency at a high enough power that the two signals cancel one another out. In the United States, currently only federal agencies are legally allowed to jam public airwaves (not individual prisons outside the Federal Bureau of Prisons system). Because of these restrictive policies and the potential for interference with legitimate emergency communications, the use of jamming technologies may not be feasible. Micro-jamming technologies are illegal in the United States, while both managed access and cell phone grabbing systems technologies are expensive, require continuous upkeep, and are unable to readily adapt to technological advances in cell phones,[17] which could render them obsolete within months of being implemented. Moreover, inmates' creativity to overcome restrictions to cell phone use cannot be underestimated as they have both the time and motivation to counter techniques correctional officials deploy.

A continuing limitation of all disabling devices is that they restrict only cellular transmissions. Even if these systems completely and reliably restrict inmates' use of cell phones, the phones would still be able to provide audio-visual recording and data storage capabilities and through physical transfer of a phone or SIM card would enable communication.

15. Grommon, E., Carter, J. G., Frantz, F., & Harris, P. (2016, September). *A case study of Mississippi State Penitentiary's managed access technology*. Document No. 250262. Rome, NY: Engility Corporation. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/250262.pdf
16. Tibbitt, A. (2016, May 25). *Prisoners outwit £1.2m mobile phone blocking technology*. The Ferret [online]. Retrieved from https://theferret.scot/imsi-catcher-trial-scottish-prison-service/
17. For example, the change from 4G to 5G networks.

Technology	How It Works	Associated Issues
Managed Access Systems	• Picks up and manages all calls made within geographic area (correctional facility) • Calls to/from approved phone numbers are allowed, while calls to/from unapproved devices are blocked • Effectively demonstrated in the United States in multiple correctional facilities, including the Lee Correctional Institution in Bishopville, S.C.	• Requires individual agreements with cell carriers for each cell phone frequency • Expensive: up-front costs range from $200K-$1M • Requires routine management (not just plug-and-play) • Requires routine maintenance of signal strength to avoid signal bleed-over and enable optimal coverage • Affected by cell phone technology upgrades (no longer effective if/when cell phone technology changes) • Vulnerable to sabotage by inmates or unscrupulous staff • Phones may still be used for pictures, voice, and video recording
Cell Phone Grabbing	• Cell phones attracted to a fake network so they can be monitored or blocked • Calls to/from approved phone numbers allowed to connect (i.e., whitelist of numbers)	• Use has been challenged in the United States because of privacy concerns[18] • Restricted catchment area is problematic in more dense, urban areas • Expensive: approximately $1.5M • Phones may still be used for pictures, voice, and video recording • Trialed in Scotland with limited success because of inmate countermeasures
Micro-Jamming Systems	• Blocks mobile reception entirely by disrupting phone signals within a very precise area	• Limited in use–only federal agencies legally allowed to jam public airwaves • Blocks both legitimate/emergency communications and illicit calls • Cost is unclear • Vulnerable to sabotage by inmates or unscrupulous staff, which would be impossible to detect if sporadic • Phones may still be used for pictures, voice, and video recording

Figure 10: Disabling solutions can interrupt the transmission of cellular signals within a correctional facility.

18. Electronic Frontier Foundation. (n.d.). *Street-level surveillance*. Retrieved from https://www.eff.org/pages/cell-site-simulatorsimsi-catchers



Limitations of Cell Phone Interdiction Methods and the Future

As with other contraband detection technologies, there are limits to what current cell phone technologies can detect and manage. Traditional X-ray and metal detection technologies cannot distinguish the presence of cell phones from other objects containing metal. Among the newest on-site cell phone detection technologies, FMD requires that the device be within close proximity to a cell phone to successfully identify its presence and can easily confuse the presence of cell phones with that of other electronics. Meanwhile, RFD can identify phones from a distance, but only when they are actively engaged in a call. Needing the phone to be active is a notable weak point in RFD capability.

Indirect disabling technologies can inactivate cell phones by using managed access systems, cell phone grabbing, or jamming solutions, but these technologies have limitations, most notably cost. These systems can cost up to $3,000,000 to deploy, with annual maintenance costs of up to $500,000. Effective use of these solutions typically involves constant configuration and adaptation to technology advances used by those involved in the contraband "market." Not only are these disabling solutions extremely expensive, but the software that powers them also requires regular maintenance, technical updates, and considerable infrastructure requirements.

A central challenge to cell phone disabling technologies is its focus on cellular communications. None of the disabling solutions keep the phones from functioning as a recording and data storage device. Only contraband management that involves finding and physically removing phones and components can successfully keep cell phones from being used in correctional facilities. Corrections administrators continue to need low-cost, wide-distance devices for on-site detection that can adapt with changing cell phone technology.

Inmate desire for unmonitored, unlimited, and low-cost communication with family, friends, and accomplices, as well as access to internet websites and social media, is expected to continue; therefore, their demand for cell phones will remain strong. Because cell phones will continue to have increased connectivity via distributed devices in the environment that are connected via the internet (i.e., the Internet of Things), cell phones will continue to offer users additional capabilities. Inmates might use cell phones to control any range of external items from their phones, such as disabling car locks, controlling lights or temperature in someone's home, or monitoring in-home security cameras. This kind of remote access could further expand an inmate's ability to manipulate or intimidate others outside of the facility.

Constant changes in cell phone technology and inmates' relentless efforts to exploit vulnerabilities in solutions aimed at detecting or restricting the use of contraband cell phones force corrections administrators to continually deploy a multilayered approach, and update detection and mitigation strategies for cell phones and componentry. With an emphasis on artificial intelligence and machine learning in every aspect of technological innovation, it is expected that more traditional X-ray and metal detection technologies may improve through the introduction of software that reduces the need for human interpretation of images.[19] It has also been posited that the introduction of next-generation SIM cards,[20] including embedded SIM (eSIM) and multinetwork SIM cards, may disrupt the traditional functionality of cell phones, because the devices can be manufactured to be smaller and to toggle between various networks, which may further challenge detection and disabling technologies within a correctional facility.

19. Department of Homeland Security. (2020, September 9). *Feature article: S&T's transportation security laboratory evaluates artificial intelligence and machine learning technologies*. Retrieved from https://www.dhs.gov/science-and-technology/news/2020/09/09/feature-article-st-tsl-evaluates-artificial-intelligence

20. GSMA. (n.d.). *The SIM for the next generation of connected consumer devices*. Retrieved from https://www.gsma.com/esim/

Three Key Considerations for Leaders in the Corrections Community

1. A multilayered system of defense is warranted to provide effective cell phone interdiction in a correctional facility to systematically manage the flow and use of cell phone contraband.
2. SIM card exchanges are increasingly becoming a means of communication that circumvents the need for cellular communication. When cellular communication is circumvented, cell phones and SIM cards are no longer manageable using indirect disabling techniques, nor can they be reliably detected using RFD and metal detection devices.
3. Currently, no disabling technologies provide a comprehensive technical solution. Current technologies in this space work well in theory (high efficacy) but often have limitations when applied to the real-world setting of a high-security correctional facility (low effectiveness).

Corrections leaders must deploy technologies to deter contraband cell phone use that fit their agency operational use case. For smaller facilities, mass shakedowns of housing units and recreation areas using metal detectors or FMDs may sufficiently deter cell phone use. For larger institutions with high numbers of cell phone confiscations, physical search methods combined with disabling technology may provide the most effective countermeasure. Regardless, corrections leaders must take action, deploy workable detection technology, and combat the major institution security threat that contraband cell phones represent in today's world of correctional facilities.

Published: **May 2021**

More Information

Steven Schuetz
Senior Science Advisor/Physical Scientist
National Institute of Justice
U.S. Department of Justice
Steven.Schuetz@usdoj.gov
Tel +1-202-514-7663

Jeri D. Ropero-Miller, PhD, F-ABFT
Project Director, CJTEC
RTI International
jerimiller@rti.org
Tel +1-919-485-5685

Neal Parsons
Research Forensic Scientist
RTI International
mparsons@rti.org
Tel +1-919-541-6000

Suggested Citation

Parsons, M. N., Lissy, K., Camello, M., Dix, M., Craig, T., Planty, M., & Roper-Miller, J.D. (2021). *Detecting and managing cell phone contraband*. National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. https://cjtec.org/

CJTEC would like to thank Joe Russo, Program Manager at the University of Denver, for his valuable efforts in reviewing this document.

This publication was made possible by Award Number 2018-75-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

https://cjtec.org/