RESEARCH REPORT

Interdiction Technologies and Strategies for Contraband Cell Phones

Bryce Peterson
CNA
July 2022

KiDeuk Kim
URBAN INSTITUTE

Rochisha Shukla
URBAN INSTITUTE

Megan Kizzort
URBAN INSTITUTE
ABOUT THE URBAN INSTITUTE

The nonprofit Urban Institute is a leading research organization dedicated to developing evidence-based insights that improve people’s lives and strengthen communities. For 50 years, Urban has been the trusted source for rigorous analysis of complex social and economic issues; strategic advice to policymakers, philanthropists, and practitioners; and new, promising ideas that expand opportunities for all. Our work inspires effective decisions that advance fairness and enhance the well-being of people and places.
## Contents

Acknowledgments iv

**Interdiction Technologies and Strategies for Contraband Cell Phones** 1

- **Contraband Interdiction** 1
- **Detection Technologies** 3
  - **Drone Detection Systems** 4
- **Disabling Technologies** 4
  - **Managed Access Systems** 5
  - **Jamming and Micro-Jamming** 5
  - **Standardized Protocols** 6
- **Nontechnological Strategies** 7
- **Conclusion** 7

**Notes** 9

**References** 11

**About the Authors** 14

**Statement of Independence** 15
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/fundingprinciples.

We would like to thank Jesse Jannetta and Janine Zweig from the Urban Institute for reviewing and providing feedback on this report.
Interdiction Technologies and Strategies for Contraband Cell Phones

Contraband is any material or item that is unauthorized by the administration of a prison or jail and poses a threat to the safety, security, or good of an institution (Kalinich and Stojkovic 1985). Of the numerous types of contraband items found in prisons and jails, cell phones have become a particular concern for administrators (ASCA 2012), with an average of 31 devices recovered per prison based on a 2018 survey (Peterson et al. 2021). Incarcerated people have used cell phones to communicate with criminal associates and organize illicit activity inside facilities (e.g., escapes, riots, assaults, drug and contraband smuggling) and outside them (e.g., homicides, kidnapping, drug trafficking, fraud, extortion, witness intimidation, harassment, child pornography, phone scams). For example, dozens of people involved in prison gangs operating within the California Department of Corrections and Rehabilitation system were charged with homicides, smuggling drugs, and other crimes facilitated by contraband cell phones. Similarly, a 2018 riot in a South Carolina Department of Corrections prison was incited in part over access to contraband phones and resulted in the deaths of 7 incarcerated people and injuries to 17 others. In this report, we discuss the strategies prison and jail administrators have implemented to interdict contraband cell phones.

Contraband Interdiction

Contraband cell phones compromise safety and security, facilitate violence, perpetuate underground economies, and shift the balance of power in prison and jail social systems. They may enter facilities externally by being brought in by visitors (Siennick, Mears, and Bales 2013), thrown over fences, or flown in on drones (Craig, Russo, and Shaffer 2016; Inch 2018). They can also be brought in by staff working inside facilities, which can be lucrative; some staff have earned hundreds of dollars per phone. In addition, staff may form inappropriate relationships with incarcerated people in which they supply them contraband or may be bribed or convinced to do so (Allen and Bosta 1981; Henry 1999; Marquart, Barnhill, and Balshaw-Biddle 2001; Worley, Tewksbury, and Frantzen 2010). Importantly, the willingness of correctional staff to smuggle contraband is linked to negligent supervision, low pay, high turnover, poor recruitment standards, and insufficient training (Capano et al. 1987; McCarthy 1981; Petherick, Turvey, and Ferguson 2009).
To combat the introduction and use of contraband cell phones in prisons and jails, administrators employ a range of technological interdiction solutions to detect them (i.e., identify their location in a facility) or disable them (i.e., render them inoperable to their users). Table 1 summarizes some of these interdiction technologies. These technologies can be categorized as active (meaning they emit radio frequency, or RF, energy), passive (meaning they only receive RF energy), or a hybrid of the two. Further, the primary function of these technologies is either to detect and facilitate the confiscation of illicit devices or disable devices and prevent their use. Nearly all the technologies listed in table 1 require substantial on-site monitoring and adjustment to be effective. Some only work when wireless contraband devices are on and in use (for instance, when being used to make calls), whereas others work even when devices are off. Most of these solutions are being used in facilities across the country, though jamming and standardized protocols have only been piloted in select facilities.

**TABLE 1**

<table>
<thead>
<tr>
<th>Technology solution</th>
<th>Type</th>
<th>Primary function</th>
<th>Phone status</th>
<th>Estimated cost</th>
<th>Legal</th>
<th>Carrier agreements</th>
<th>Locations (select)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Body scanners</td>
<td>Passive</td>
<td>Detect</td>
<td>On or off</td>
<td>$150–300K (facility)</td>
<td>Yes</td>
<td>No</td>
<td>AL, FL, NH</td>
</tr>
<tr>
<td>Body Orifice Security Scanner chairs</td>
<td>Passive</td>
<td>Detect</td>
<td>On or off</td>
<td>$12,000 (unit)</td>
<td>Yes</td>
<td>No</td>
<td>CA, GA, TX</td>
</tr>
<tr>
<td>Detect/locate systems</td>
<td>Passive</td>
<td>Detect</td>
<td>On or in use</td>
<td>$300,000–1.5M (facility)</td>
<td>Yes</td>
<td>No</td>
<td>PA, BOP, SC</td>
</tr>
<tr>
<td>Drone detection systems</td>
<td>Passive</td>
<td>Detect</td>
<td>On or off</td>
<td>$50,000–$400,000 (facility)</td>
<td>Yes</td>
<td>No (may require FAA coordination)</td>
<td>Pilot tests and acquisition ongoing</td>
</tr>
<tr>
<td>Handheld ferromagnetic</td>
<td>Passive</td>
<td>Detect</td>
<td>On or off</td>
<td>$500–$1,500 (unit)</td>
<td>Yes</td>
<td>No</td>
<td>Most jails and prisons</td>
</tr>
<tr>
<td>Handheld radio frequency detectors</td>
<td>Passive</td>
<td>Detect</td>
<td>On or in use</td>
<td>$500–$2,500 (unit)</td>
<td>Yes</td>
<td>No</td>
<td>NJ, PA</td>
</tr>
<tr>
<td>Jamming solutions</td>
<td>Active</td>
<td>Disable</td>
<td>On or in use</td>
<td>$1.5–$2.5M (facility)</td>
<td>Federal only</td>
<td>FCC/legal approval</td>
<td>BOP currently testing</td>
</tr>
<tr>
<td>Managed access systems</td>
<td>Passive/hybrid</td>
<td>Disable</td>
<td>On or in use</td>
<td>$1.2–$5.0M (facility)</td>
<td>Yes</td>
<td>Yes</td>
<td>CA, MD, MS, TX</td>
</tr>
<tr>
<td>Nonlinear junction detection</td>
<td>Active</td>
<td>Detect</td>
<td>On or off</td>
<td>$15,000 (unit)</td>
<td>Yes</td>
<td>No</td>
<td>TN</td>
</tr>
<tr>
<td>Standardized protocols</td>
<td>Active</td>
<td>Disable</td>
<td>On</td>
<td>$100,000 (facility)</td>
<td>No</td>
<td>FCC/legal mandate</td>
<td>None</td>
</tr>
<tr>
<td>Transportable ferromagnetic</td>
<td>Passive</td>
<td>Detect</td>
<td>On or off</td>
<td>$7,200–$10,000 (unit)</td>
<td>Yes</td>
<td>No</td>
<td>Most jails and prisons</td>
</tr>
</tbody>
</table>

Source: Urban research team.

Notes: BOP = Bureau of Prisons. FAA = Federal Aviation Administration. FCC = Federal Communications Commission. "Facility" refers to the cost of implementing the technology for an entire prison or jail, while "unit" refers to the price for a single unit of the technology (e.g., the price for a single handheld metal detector).
Detection Technologies

There are several wireless interdiction technologies whose primary function is to detect contraband cell phones. These include the following:

- **Body Orifice Security Scanners**, or BOSS chairs, are a type of ferromagnetic detector designed to find contraband in multiple areas of the body of someone who sits on it.

- **Body scanners** are similar to metal detectors but can detect a variety of items on a person’s body, including nonmetallic objects. They typically use high-frequency radio waves to produce a three-dimensional image of a person and identify items under their clothes or in body cavities. Staff typically use these on incarcerated people entering or reentering a facility and on other staff before they start their shifts.

- **Detect/locate systems** combine RF detection with a software that determines the location of a phone in use. These systems require a network of sensors placed throughout a facility and thus have broader functionality and range.

- **Handheld ferromagnetic detectors** or “wands” are small versions of ferromagnetic detecting technologies. Staff use these to search people entering facilities and to search cells and other areas that are not easily accessible.

- **Handheld RF detectors** detect radio signals emanating from wireless contraband devices. Staff use RF detectors to “sweep” facilities to find cell phones people are currently using.

- **Nonlinear junction detection technologies** detect cell phones using the semiconductor junctions found in electronics.

- **Transportable ferromagnetic detectors** are metal detectors optimized to detect cell phones via their ferromagnetic components. Staff primarily employ these to find phones that may be concealed on a person or in a facility. These detectors are installed at facilities’ entry and access points (e.g., intake areas or doors to recreation areas) so people must walk by them as they enter or move through facilities.

Shaffer and Russo (2015) have conducted the most comprehensive test and evaluation of handheld wireless interdiction technologies. They assessed four different technologies: two RF detectors, one ferromagnetic detector, and one nonlinear junction detector. They found that the RF detectors were consistently accurate at detecting an active phone call in the facility, had long-range capabilities (detection from up to 125 feet), and triggered no false alarms during testing. However, the RF detectors provided no utility in finding cell phones that were turned off. Conversely, the ferromagnetic detector and the nonlinear junction detector were able to locate phones that were turned off, but only those in very close proximity (0 to 8 inches). The ferromagnetic detector and the nonlinear junction detector
also had high false alarm rates (28 to 76 percent). Because of these false alarms and the limited range of the devices, staff strongly preferred the RF detectors (Russo 2016; Shaffer and Russo).

**Drone Detection Systems**

There are also interdiction technologies that detect drones that may be introducing contraband into a facility. The use of this emerging technology stems from growing concerns among correctional officials that drones are being used to bypass traditional contraband interdiction strategies to deliver contraband items, including cell phones (see Shukla, Peterson, and Kim 2021 for an example with pictures of a drone dropping several phones into a Florida prison). In 2018, the Federal Aviation Administration instituted new rules that restrict flight over federal prisons and Coast Guard facilities. Many correctional agencies have begun testing and implementing drone detection technologies (see Inch 2018) that can determine when a drone is flying over a facility. These technologies typically work by identifying the RF signals between the drones and their operators and alerting officials within the facility. This can help staff intercept contraband being delivered via drone and, when possible, aid in the apprehension of the drone operators. Likewise, some agencies are exploring the use of radar technology to identify and prevent people from approaching a facility to throw contraband over the fence or fly it over on a drone.

Though drone detection systems show promise for detecting most drones currently on the market, this technology is nascent and there is no research demonstrating its effectiveness. In addition, the full-scale implementation of drone detection systems is susceptible to technological challenges (e.g., trouble identifying specific RF frequencies) and legal hurdles (fourth amendment concerns about intercepting RF frequencies, geolocation, and other data from the drones or operators).

**Disabling Technologies**

Whereas the technologies described above are designed to detect phones inside a facility or before they are introduced to one, other interdiction solutions are designed to disable phones to prevent their use by incarcerated people. These include managed access systems, jamming technologies, and standardized protocols.
Managed Access Systems

A managed access system (MAS) is designed to capture and block cell phone transmissions by establishing its own private cellular network within a designated space. It may interface with commercial cellular infrastructure to allow whitelisted and emergency phone calls to be routed. An MAS checks the identifying information of devices transmitting cellular signals and permits transmissions from approved devices to communicate with commercial networks while terminating those from nonapproved devices (FCC 2017). Two studies funded by the National Institute of Justice found that MASs can be effective at reducing illicit phone calls in facilities, especially when combined with other policy changes (e.g., increased or enhanced searches) and larger penalties for the possession of a contraband cell phone (Frantz and Harris 2016; Grommon et al. 2016). One study in Mississippi found that an MAS detected 544,141 attempted calls from 2,260 devices during the study period (January to April 2012), even though only 257 phones were confiscated during that period (Grommon et al. 2016).

Despite promising research evidence for MASs, the technology has noteworthy limitations. Installing an MAS requires new infrastructure consisting of numerous transceivers and antennas, making it expensive and logistically difficult to implement and maintain one on a large scale (CCST 2012). The cost of installing an MAS, dedicating resources to negotiate with the wireless carriers in the area, and actively monitoring the system once it is set up could exceed $1 million for a medium-sized facility. Moreover, MASs only intercept cellular communications and do not disable cell phones’ other capabilities, such as Wi-Fi connectivity, computing, and photographic/video functions (Frantz and Harris 2016), meaning incarcerated individuals can still use them to record videos or connect to other networks. Furthermore, there is uncertainty around MASs’ effectiveness at intercepting unauthorized text messages or preventing incoming calls because of the time it takes them to detect and terminate illicit transmissions (CCST 2012).

Jamming and Micro-Jamming

The detection systems and MASs described above have all been implemented in numerous states and facilities. A few technological strategies are emerging that have yet to be fully implemented in the United States but show promise for effectively disabling contraband wireless devices. One such technology is jamming, an RF-based technology that disrupts cell phone signals within a specific geographic area (Scism and Sterling 2008). Unlike MASs, jamming does not discriminate between
authorized and unauthorized devices, nor does it require facilities to work with phone carriers; rather, this solution disables all cellular communications within a target area.

Even though jamming has broad support among correctional administrators,\textsuperscript{11} the Communications Act of 1934 prohibits state and local corrections officials from employing it (Fitzgerald 2010). The Federal Bureau of Prisons, however, is exempt from that act and in early 2018 piloted a micro-jamming technology in its Federal Correctional Institution Cumberland facility (Inch 2018).\textsuperscript{12} The South Carolina Department of Corrections has also tested jamming technology under a deputization agreement with the BOP.\textsuperscript{13}

There are several potential issues with jamming. First, it is expensive. New Zealand spent nearly $7.8 million ($11.37 million NZD) to install jammers in its prisons between 2007 and 2009.\textsuperscript{14} To put this in perspective, the number of sentenced individuals in New Zealand's correctional system was 8,244 as of December 2009.\textsuperscript{15} Like MASs, another criticism is that jamming does not disable phones' other functions (e.g., video recording and Wi-Fi connectivity). For example, even though New Zealand has had jammers in all of its prisons for a decade, incarcerated people have continued to post pictures and videos on social media from contraband phones.\textsuperscript{16} Finally, an important concern is that jamming will leak out of a facility and disrupt calls made by the public or interfere with emergency response radio systems.\textsuperscript{17} After Brazil installed a jammer in one of its prisons, the cell service of 200,000 nearby residents was disrupted.\textsuperscript{18}

**Standardized Protocols**

Another emerging technological solution is the installation of standardized protocols on the firmware of cell phones. After installing these protocols, an agency would place a series of short-range sensors in strategic locations throughout a facility. When a wireless device is within range of a sensor, it is completely disabled (NTIA 2010). For an agency to fully implement this technology, it would need regulatory assistance from the Federal Communications Commission and compliance from the wireless carriers and cell phone manufacturers. This technology has only been tested in laboratories and is not yet being used in any facility; there also are concerns from wireless companies that this technology would be susceptible to cybersecurity vulnerabilities (Saunders et al. 2017).

Although information on their effectiveness is limited, the technical features of standardized protocols are unique. Unlike other existing and emerging technologies (e.g., detection devices, MASs, jamming), standardized protocols would be relatively inexpensive to install and maintain, disable all cell phone functions (not just calls/communication), work on all phones and carriers, and would not
interfere with carrier frequencies.\(^{19}\) Support for this technology is growing among corrections professionals and administrators (Saunders et al. 2017).\(^ {20}\)

### Nontechnological Strategies

In addition to the technologies outlined above, facilities use nontechnological solutions to combat contraband, such as management practices (ASCA 2012), as well as hiring, training, and retaining quality staff (see Russo and coauthors 2022 for an overview of these nontechnological approaches to contraband cell phone interdiction). For example, officers search visitors, staff, and incarcerated people for unauthorized items (Duncan 2008) using methods ranging in intrusiveness from visual scans to body cavity searches, and they may be assisted by K-9 units trained to detect cell phones.\(^ {21}\) Similarly, some agencies have installed netting over facility walls (Peterson et al. 2021) to prevent contraband from being thrown in.

Other approaches to cell phone interdiction focus on reducing their demand among incarcerated people. For example, many facilities have begun providing tablets or other communication devices to their incarcerated populations. It is possible that access to these devices can curb the demand for illicit phones. Likewise, many states have expanded visiting and other administrative practices focused on improving overall connections between incarcerated people and their loved ones (see Peterson and coauthors 2019 for an overview of such practices).

States have increased criminal penalties for smuggling or possessing contraband phones to deter their introduction and use. For example, in 2008 Florida passed a law that made the possession of phones in prison a felony. Mississippi law prohibits the possession of a cell phone in prison, which carries a penalty of 3 to 15 years in prison and a $25,000 fine, and people (including staff) who assist in the delivery of a contraband cell phone may be prosecuted. There are similar laws in place in most states and at the federal level.

### Conclusion

Contraband cell phones pose a threat to the security of prisons and jails and to the safety of incarcerated people, correctional staff, and the public. The technologies we describe in this report, which include those designed to detect or disable wireless devices, are among the many solutions correctional administrators can implement to combat contraband cell phones. Despite the widespread
availability and use of these technologies in correctional settings, there has been little empirical research on their efficacy and officials do not yet know what returns they can expect on their investments of resources and staff. Thus, there is a critical need for correctional agencies to collect more data and partner with researchers to better understand the degree to which these technologies can prevent the use of illicit cell phones and thereby prevent harm to people inside and outside facilities.
Notes


8. For a more comprehensive list of vendors and models of detection devices, see Koslover and coauthors (2017).

9. All cell phones have ferromagnetic components. Simply put, ferromagnetism is a type of magnetism exhibited by some of the components found in cell phones.

10. Linthicum and Gondles, Jr., letter to Marlene H. Dortch regarding the American Correctional Association’s comments on combating contraband wireless device use in correctional facilities; Gondles, Jr., “Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities.”


Shadwell, "Jail 'Fight Club' Filmed on Cellphone Despite Multimillion-Dollar Jammers."

Burke and Owen, "Cell Phones as Prison Contraband."


Try Safety First white paper on contraband cell phones, accessed June 6, 2022 (not available online).

Linthicum and Gondles, Jr., letter to Marlene H. Dortch regarding the American Correctional Association’s comments on combating contraband wireless device use in correctional facilities.

Burke and Owen, "Cell Phones as Prison Contraband"; Binetti (2008); FDLE (2014); Kannenberg (2003); NLETC (2013); Prendergast and coauthors (2004).
References


About the Authors

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, 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 research associate in the Justice Policy Center at the Urban Institute, 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.

Megan Kizzort is a policy program associate in the Justice Policy Center at the Urban Institute, where her work focuses on criminal case processing and correctional technology. Before joining Urban, Kizzort completed an MS in public policy and management at Carnegie Mellon University and worked as a program analyst in the Criminal Division of the US Department of Justice.
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.