Digital System, Evidence & Forensics Issues In Correctional Environments

Natalie Armstrong
Department of Forensic Psychology
Marymount University
Arlington, Virginia, U.S.A.
natalie.e.armstrong@gmail.com

Michael Losavio
Department of Justice Administration
University of Louisville
Louisville, Kentucky, U.S.A.
michael.losavio@louisville.edu

Deborah Keeling
Department of Justice Administration
University of Louisville
Louisville, Kentucky, U.S.A.
deborah.keeling@louisville.edu

Abstract - The correctional environment is one of the most controlled in the United States. Despite the regimented system that epitomizes correctional facilities, digital systems have entered that environment as contraband and data backchannels subject to compromise that threaten control of institution and the effectiveness of incarceration for the incapacitation of offenders. We examined data on this issue and possible solutions.

Keywords-digital, forensic, corrections, jail, prison, parole, probation

I. INTRODUCTION

In December, 2009, former jail inmate Francis Janosko was sentenced to 18 months imprisonment for hacking the computers at the Plymouth County Correctional Facility *while incarcerated there*. [1] During the colloquy to establish facts sufficient to support his plea of guilty to the federal offense of unauthorized access to a computer, the prosecution related that

> …while JANOSKO was an inmate at the Plymouth County Correctional Facility in 2006 and 2007, the correctional facility provided inmates a computer for legal research with security controls to prohibit Internet access, e-mail, or using other computers or computer programs. Despite these restrictions, JANOSKO hacked the computer network to send e-mail; to provide inmates access to a report that listed the names, dates of birth, Social Security numbers, home addresses, telephone numbers and past employment history of over 1,100 current and former Plymouth County Correctional Facility personnel and applicants; and to access (without success) an important prison management computer program. [1]

Pervasive and ubiquitous use of digital communications devices carry threats to the security of the last stage of criminal justice process: the prisons and other correctional institutions charges with the incapacitation of criminal offenders found guilty of crimes. The failure of information control of convicted offenders is both an internal threat to the institution and an external one for the victims, witnesses and law enforcement personnel whose lives they may touch through that data channel.

Communication devices in prisons, from computers to cell phones, are an opportunity for uncontrolled data activity and coordination with people on the outside. These activities may include intentions to run a criminal enterprise, intimidate a witness or victim, or plan an escape.

978-0-7695-4052-8/10 $26.00 © 2010 IEEE
DOI 10.1109/SADFE.2010.22

The growing power of cell phones pushes their usefulness far beyond their original intent; rather than simply being a portable form of communication, they have evolved into micro-computers capable of many of the same abuses of a full sized computer. The shrinking size of cell phones has made them easier to hide and more difficult to confiscate. The problem will only expand as more and more features are incorporated in smaller and smaller hand-held devices designed to connect with other computing and communication systems.

Several of these handheld devices now provide telephony, Internet connectivity and viewing, music/video reception and viewing, and GPS mapping right to the user. Yet even general and special purpose computers pose issues that correctional staff must address, such as contraband data held and hidden on otherwise innocuous media like game CDs or cartridges.

A.Pervasiveness & Scope

Controlling contraband cell phones and personal data assistants may be as difficult as with any contraband items. Contraband cell phones in prisons are serious issues in corrections. [2] North Carolina Corrections recovered over 140 cell phones in its institutions in 2008, where the going price for a cell phone was up to $500.00; Texas recovered more than 700, of which 20 were seized from death row inmates. [3] A Tennessee inmate used one to plot his escape, while other inmates used them to arrange attacks on inmates and harass victims. [3] Others assert gangs coordinate activities from prisons with smuggled cell phones. [4]

Unfortunately, the scope of the problem is not confined solely to cell-phones. Computers with Internet services are now found in prisons, just as with offices and schools. Inmates may have access as part of their prison employment, inmate legal research, or education. One example is a former governor of Louisiana, serving time in federal prison, had an e-mail newsletter that dismayed officials for its criticism of correctional cuisine.

Perhaps it comes as little surprise that these systems have been used to access and collect contraband information, often pornography.

II. SYSTEMATIC EXAMINATION OF THE DIGITAL EVIDENCE AND FORENSICS ISSUES IN CORRECTIONS

An anonymous survey was done to pilot an examination of this issue beyond anecdotal accounts. This survey was taken of conference attendees during a session on digital evidence issues for the Kentucky Council on Crime and Delinquency in September, 2008 The sample, N=16 consisted of personnel working in maximum and non-maximum adult facilities, juvenile facilities, probation and parole supervision and "other," (See Figure 1 for a distribution of the participants' occupations within corrections).

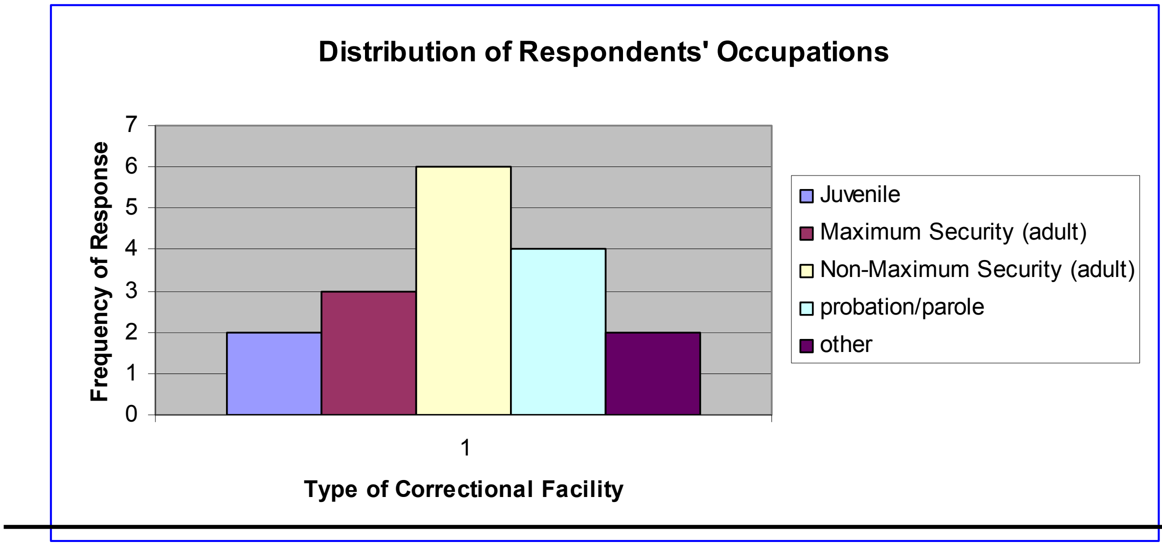

Figure 1 – Distribution of Respondents by Correctional Facility/Occupation

Due to the reduced sample size and qualitative nature of the data collected, frequency statistics were utilized. Table 1 lists the frequencies of the data the authors deemed most apt to illuminate the issues at hand. The data suggests that the individuals sampled were largely aware of the misuse of electronics by inmates in their institutions (52.9%).

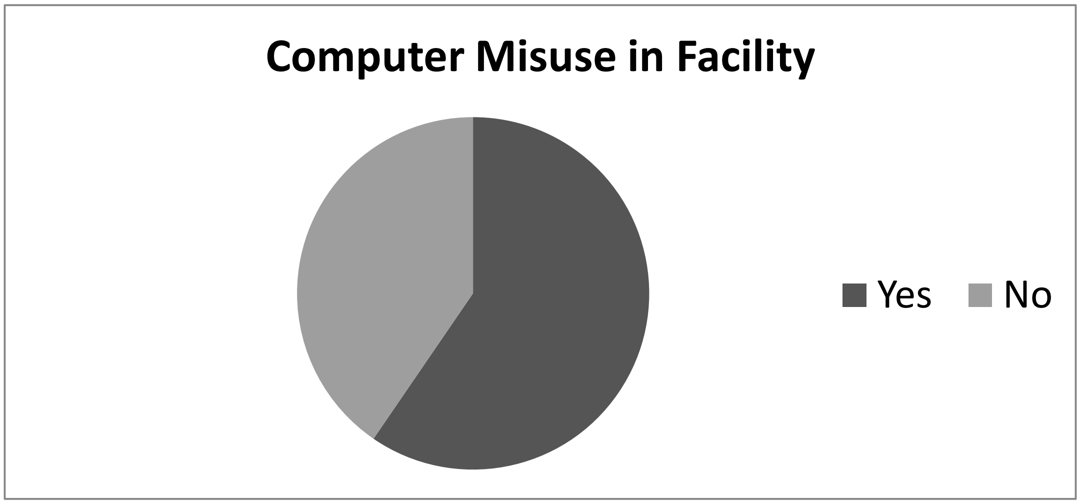

Figure 2 – Percentage of Respondents Who Experienced Computer Misuse in Their Correctional Facilities.

However, when asked to answer whether they had encountered specific types of computer misuse, such as hacking encrypted information, and recognizing illegal use of web-based email and internet use 64.7% and 47.1% respectively, responded "No."

Also of particular interest was that the participants rarely responded to the problem by employing forensic analyst (5.9%), or to have the issue analyzed at all (23.5%).

According to the respondents, it does not seem to be an issue of cost, as all but two respondents stated that cost was not an issue in whether or not an inquiry into misuse of electronics was aborted.

Even when accounting for the reduced sample size and dichotomous response style of the questionnaire, it is clear that further inquiry is needed to further discern the awareness of the respondents to electronic misuse, as well as what steps are being taken should misuse be discovered.

Frequency Table for Pilot Data Questionnaire

	Frequency	Percent
You work in		
Correctional facility (juveniles)	1	5.9
Non-maximum security adult facility	4	23.5
Maximum security adult facility	4	23.5
Probation/parole	4	23.5
Other (not-specified)	3	17.6
Have you ever experienced (in your facility):		
Computer misuse		
Yes	9	52.9
No	6	35.3
Encrypted computer information misuse		
Yes	4	23.5
No	11	64.7
Internet email misuse		
Yes	7	41.2
No	8	47.1
Internet web viewing misuse		
Yes	7	41.2
No	8	41.7
Locked/encrypted information (general)		
Yes	1	5.9
No	14	82.4
Do you anticipate new issues?		
Yes	4	23.5
No	6	35.3
Have you ever had your computer analyzed for suspected misuse?		
Yes	4	23.5
No	12	70.6
Was it by a Forensic Analyst?		
Yes	1	5.9
No	9	52.9
Did you find evidence of misuse?		
Yes	4	23.5
No	5	29.4
Have you ever had to give up an inquiry into misuse of electronics because of cost?		
Yes	0	0.00
No	10	58.8

N = 16

Table 1 – Frequency Table for Pilot Data Questionnaire

III. SOLUTIONS

Addressing this for correctional institutions requires attention to all three subdomains of information security: legal, administrative and technical.

A. Legal & administrative

Legal restrictions may be effective if the subjects are aware of those restrictions and, subsequently, are deterred by them. A central issue with "cyberlaw" is that many people simply are not aware of pertinent laws prohibiting certain kinds of conduct with electronic devices. There is neither tradition nor pedagogy on good computing practice.

The Arizona legislature banned inmates from direct and indirect access to Internet web sites, the most extreme ban in the United States. Banning indirect access means an inmate cannot even access web site information through a third party, such as an associate outside the prison.

Putting aside rights of access to information, such a solution might work with typical computer systems within a facility. It may leave an inmate unprepared for many types of jobs upon release, but as an absolute bar it should stop such misconduct within a prison. Whether or not it will help with indirect access outside the facility is problematic, since these may also be the most easily monitored computers inside. Tracking and forensic software on prison systems can catch most improper activity and alert to the use of anti-forensic technologies by inmates.

Even if generally aware, people may still not comply, as seen in the continued practice of downloading music and video in violation of copyright law. For prison inmates, the deterrent effect of law may be even more attenuated. Some states have moved forward with special felony penalties for those both supplying and possessing contraband cell phones in prison in an effort to dissuade inmates and their suppliers outside prison walls. Yet such controls have been insufficient; for example, despite the prohibitions and penalties on possession of contraband cell-phones, one inmate's mother called his warden to complain about the bad cell phone reception she experienced during her conversation with her son. [5]

Administrative restrictions, when enforced, may be more effective as they may more clearly explain what is prohibited and may more immediately enforce those prohibitions. Training and enforcement are key elements to make any such administrative measures effective. But this works best for negligent or unintended breaches of security; for those intent on forbidden activity, administrative restrictions may be of only limited benefit.

B. Technical

Technical solutions face special hurdles with these radio-frequency devices independent of control by any institution other than the service provider. Their use and monitoring is subject to extensive federal regulation. FCC regulations generally prevent cell phone signal jamming, although there are limited, high-security exceptions for federal agencies, though legislation is pending to expand that to state entities. The Wiretap Act requires judicial approval to intercept and monitor cell phone transmissions. Broadcast signal jamming and signal interception, as a practical matter, might cause other problems within and without the institution.

Interestingly, the olfactory prowess of our canine associates has seen success with cell phones. Institutions in the United Kingdom, Florida, South Carolina and other states use dogs trained to scent a particular component of cell phones, with some success. [6], [7] The training comes at about $6500.00 per hound. [8]

Techniques to counter these technologies are used by inmates. Cell phones, when not in use, are being disassembled and distributed around the facility, making these component parts more difficult to find and easier to replace when found. Removing the SIM card from the handset makes the most valuable digital forensic data easier to conceal.

Given the small size of devices and their components, any crevice may serve as a difficult-to-find hiding place. [9]

The Naval Surface Warfare Center (2006), at the request of the Federal Bureau of Prisons (FBP) and the National Institute of Justice (NIJ), examined this problem and noted that:

> Four main approaches have been identified to deal with the cell phone problem: (1) locate and confiscate cell phones through the use of detection technology; (2) overpower the cell phone signal with a stronger signal, commonly referred to as “jamming;” (3) trick the cell phone into reacting as if there is no service; and (4) intercept the signal, which requires a judge’s order. The simplest option is signal detection which carries no regulatory or legal restrictions. Since all cell phones use radio frequency (RF) antenna power, the FBP, the NIJ, and the Naval Surface Warfare Center-Dahlgren are launching a multi-year project to develop technology to detect RF and to evaluate and test existing technologies. [10]

Jamming

The brute-force, non-forensic response to contraband cell phone and other wireless device use in prisons in interference via signal transmission that renders those devices useless. “Jamming” cell phone signals and wireless signals currently runs afoul of FCC regulations and the interests of cell phone companies seeking clear signals for their systems.

But in February, 2010, with the permission of the National Telecommunications and Information Administration, the federal Bureau of Prisons began testing the use of cell phone jamming equipment at the Federal Correctional Institution in Cumberland, Maryland. [11]

At the same time, legislation is currently pending in Congress to permit the use of jamming technologies by state and local governments. This follows the submission of a petition signed by the correctional heads of 26 states requesting permission to use such systems in state prisons.

Cell phone providers continue to object to such systems, warning of interference with legitimate use and emergency response. But the evident popularity of the solution means the results of the FCI Cumberland test will closely examined.

Signal Detection

Signal detection and transmitter location may address this, though cost may be a controlling factor. Application of engineering to research problems in this area might exploit wireless E911 tracking technology and use of cell phone sensor networks.

E911 and other mobile phone tracking technologies

Tracking and general location services are available from mobile units where they signal for the closest cell tower. Each signal to the tower, regardless of the use of the phone for a call, associates the phone with the area around the tower. The signal strength and signals to other cell towers give further information as to a cell phone’s location. This creates a starting location point for the cell phone.

Enhanced 911 service was implemented to associate a physical address with an emergency 911 telephone call over a traditional wired telephone line. The system and enabling legislation allowed access and matching of caller line information to databases of caller location data. An emergency operator could then receive the location of the caller as the call was in progress.

For wireless cell phones, this type of location service doesn’t work as there is no fixed use location associated with the portable device. This has led to efforts to create a wireless enhanced 911 service to location a particular cell phone during a 911 call.

Such a system may use cell tower triangulation from the angle of arrival of cell signals between two towers. Another option uses cell tower multilateration to measure the time difference in the time of receipt of a cell signal at three or more cell receivers. Given the fixed speed of the signal, just that time difference can be used to get a location on a plane; add a fourth receiver and you can get a 3-D location. Both methods face accuracy questions, but pinpoint location may not be needed.

A review of technical and regulatory restrictions on wireless E911 could offer the relatively inexpensive solution of using it to locate cell phones in use in controlled facilities. Utility may vary with cell tower deployment in a particular area, but use of existing analysis systems for emergencies could help in the public safety context of corrections. Enabling legislation and negotiation with service providers may be necessary, but regulatory review should reveal how best to address any needs in that area.

Use of a local sensor network

These same location technologies could be applied locally through a sensor network for cell phone signals within a facility. This would avoid some of the regulatory or contract issues found in working with service providers themselves. But it requires greater resources. EVI Technology estimates a grid for a 40,000 sq. ft. area (about an acre) would require a 10-sensor network. [12] The sensors are networked to a computer which does site location and alerts in time for an effective search.

But the size of institutions may drive costs beyond their reach in these times of stretched budgets. For example, the Kentucky State Reformatory has nearly 2000 beds in its twelve dormitories and covers 43 acres. A sensor network of the entire facility might require as many as 400 sensors to be effective.

Interception of cell phone activity, either content or transactional information, may require a court order under the Wiretap and other statutes. Retrofitting a wire cage to ground and block all signals around a facility might cost too much and would block all use of radio-based systems, including those of law enforcement.

An affordable way to detect and triangulate on cell phone use within facilities may be the best solution. Using only the signal generated by the cell phone, this alerts to phone use and location with the facility in time to conduct a sweep of the area. The reduced expectation of privacy inside prisons avoids legal problems with the technology. The problem has been the cost of building a system cash-strapped correctional departments can afford.

Arrangements with cell phone companies to log activity off cell tower antennae aimed at a facility might help, given the increasing willingness of companies to share their data with law enforcement. This could be cross-indexed against handsets legally in the institution and institutional records of inmate telephone logs. But, again, there may be conflicts with federal privacy statutes and risks of infringing the privacy of ordinary citizens, depending on the location of the prison facility.

As for legal solutions, in Kentucky contraband possession of a cell phone by an inmate is a misdemeanor; only possession of “dangerous contraband” is a felony. Simple possession penalties themselves may not deter anyone other than someone nearing release.

Hybrid systems

A mixed option is also possible, with cell phone detection and jamming combined in a single device. Netline’s C-Guard Hammer system monitors for cell phone use; once a signal transaction is detected, the jamming signal is activated and the transaction disrupted. [13]

IV. FUTURE RESEARCH

Based on the pilot data collected, it is wise to continue research in this area. There are many options by which to accomplish this undertaking. Future research should examine whether or not there is a difference in occupational perception of electronics misuse.

As an example, the person who monitors the yard may not perceive electronic misuse to be an issue, either as a function of the job description, and or their personal perceptions of the severity of electronic misuse. The age of the participants should also be considered, as those with less exposure to electronics in general may not perceive the threat to be as great. The types of occupations within the facility might also produce variegated responses of the participants; as previously mentioned, a guard who works closely with the inmates may perceive the threat of misuse to be greater than, perhaps the warden, who might have more restricted access to current inmate activity. To avoid confounds of this nature, it would be wise for future research to sample the many tiers of workers in the facility.

Another method of recourse for future research would be to re-examine the types of questions posed by the questionnaire used for this paper. Because the participants responded in a way that could not be coded quantitatively, a new questionnaire should be developed to address this issue.

Moreover, the questions should be designed to pinpoint what the authors perceive to be the crucial issues, rather than just a survey questionnaire as it was in this instance.

V. CONCLUSION

Ozmint of South Carolina Corrections argues that, given the costs of signal sensor networks, signal jamming is the optimal solution as to effectiveness and cost and the best way to stop continued criminal activity by inmates; his department went so far as to conduct a demonstration project that did not impact cell traffic outside the prison. [14], [15] Yet the cell phone industry is concerned about the spill-over effects on the general public, which might create public safety issues for folks near institutions who cannot reliably use their cell phones. Momentum seems to favor this non-forensic approach, although the results of the FCI Cumberland test may find limitations on this as a technique, especially for any correctional facility not located in an isolated, rural area. Urban prisons might create a particular problem for cell phone and wireless communications in the locale.

Resolving this impasse in a cost-effective manner is important for criminal justice and public safety. The incapacitation function of corrections is undermined when inmates can continue their criminal activities; rehabilitation becomes more difficult, if not impossible. But where is the funding?

Research on sensor networks combined with research on restricted low-power jamming is a low-cost compromise that may work. Though more costly, a distributed system of low-power jammers minimizes service disruption outside the institution and may meet FCC and service provider concerns. A comparison of the two options may give guidance for correctional policy.

This area represents a unique area of research collaboration between the digital forensics community and correctional institutions, a new and nontraditional approach for DF research. For example, the Kentucky Department of Corrections and the University of Louisville are discussing collaborative options to solve this problem. That may require a combination of technical, legal and administrative solutions from across government, industry and the academy. A challenge, like all others in public safety, but an important one for the safety of law enforcement and the public.

REFERENCES

[1] USDOJ Press Release, December 22, 2009 " Former Inmate Sentenced for Hacking Prison Computer," http://www.cybercrime.gov/janoskoSent.pdf, last visited March 1, 2010

[2] Fox, A. (2006, October). A call to end contraband cell phone use. *Corrections Today*. Retrieved February 12, 2009 from http://findarticles.com/p/articles/mi_hb6399

[3] Kane, D. (2008, December 5). Cell phones plague prisons. *The News & Observer*. Retrieved February 11, 2009 from http://newsobserver.com/news/story/1321262.html

[4] *Inmates smuggle in cell phones with ease* (2006, October 12). All Things Considered. National Public Radio. Retrieved February 12, 2009 from http://www.npr.org/templates/story/story.php?storyId=6248833

[5] Hylton-Austin, H. (2008, November 26). Trying to keep cell phones out of prison. *Time Magazine*. Retrieved February 12, 2009 from http://www.time.com/time/nation/article/0,8599,1861553,00.html

[6] Murph, D. (2006, October 5). Trained dog sniffs out cellphones in prison. EngadgetMobile. Retrieved February 11, 2009 from http://www.engadgetmobile.com/2006/10/05/trained-dog-sniffs-out-cellphones-in-prison/.

[7] Florida Department of Corrections (2008, October 7). *Cell phone sniffing dog will help enforce new law*. Press Release. Retrieved February 11, 2009 from http://www.dc.state.fl.us/secretary/press/2008/dogcellphones.html.

[8] CellGeek (2008, October 7). Meet the cell phone sniffing dog. *The Cell Freak*. Retrieved February 11, 2009 from http://www.thecellfreak.com/blog/meet-the-cell-phone-sniffing-dog.

[9] *Seven prisoners in hospital after hiding cell pohnes in their bodies*. (2008, September 2). *Dial-A-Phone*. Retrieved February 12, 2009 from http://www.dialaphone.co.uk/blog/?p=2102.

[10] *No more cell phones* (2006, April). *Corrections Today, National Institute of Justice Update*. Retrieved February 12, 2009 from http://www.ncjrs.gov/pdffiles1/nij/214920.pdf

[11] "Prison to Test Cell Phone Jamming;, February 16, 2010 Wall Street Journal, http://online.wsj.com/article/SB10001424052748704804204575069774004199984.html last visited March 1, 2010

[12] Whitepaper, I.T.T. (2007, June 7). Detecting and locating cell phones in correctional facilities. Retrieved February 12, 2009 from http://www.testmart.com/webdata/mfr_pdfs/itt/White_Paper_Cell_Phones_in_Prison.pdf.

[13] Netline Cell Phone Detectors, http://www.netline.co.il/page/cell-phone_detector.aspx, last visited March 1, 2010

[14] Ozmint, J. (2009, Jan 5). Allow cell phone jamming. *Corrections.Com*. Retrieved February 12, 2009 from http://www.corrections.com/articles/20369.

[15] Kittle, Robert, *South Carolina Prison Cell Phone Jamming Demonstration Conducted,* WJBF-TV, November 22, 2008, http://www2.wjbf.com/jbf/news/science/article/cell_phone_jamming/8928/, last visited 3/1/10