Taking Back Control

The Challenges of Inmate Telephone System Security

JLG TECHNOLOGIES

PREVENTING CRIME ONE VOICE AT A TIME

Abstract

Today’s inmates are more aggressive than ever in their efforts to commit and hide crimes over inmate telephone systems. This whitepaper describes a breakthrough in corrections phone surveillance technology that “memorizes” voices of inmates over phone calls, and exposes inmates who try to abuse the system and hide their identities. Known as continuous-speech voice identification, this technology is very effective at breaking the stranglehold of crime and abuse over inmate telephone systems at corrections facilities.

Introduction

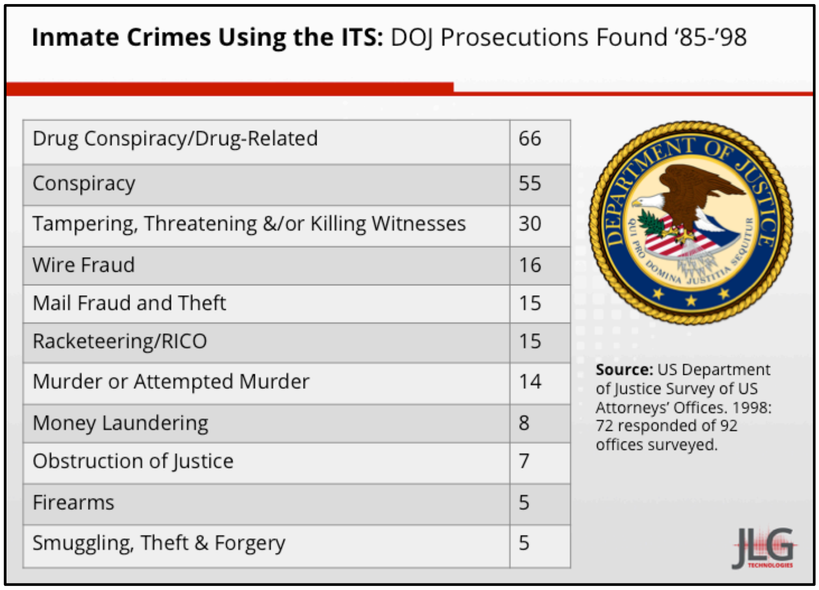
Departments of Corrections, entrusted with maintaining the safety of the states and communities they serve, face enormous challenges in controlling inmate behavior every minute the inmate telephone system is connected to the outside world.

The men and women who run these institutions work relentlessly to try to protect the public. Yet their efforts are thwarted by inmates who use the limitations of telephone system surveillance technology to hide their illegal activities.

New crimes committed over prison telephone systems by inmates are a frequent occurrence and constant threat, despite the best efforts of skilled, dedicated correctional investigators. These investigators work tirelessly to acquire a lead on an inmate suspected of telephone-related criminal activities, only to have the investigation hit a dead end. All too often the inmate buries all traces of his activities through deception and manipulation of the phone system. Inmates conspire and continue to commit murder and other serious crimes, escape from prison, engage in dangerous gang-related activities, deal in drugs, run credit card scams, smuggle contraband into correctional facilities, and intimidate victims and witnesses. For these inmates the telephone system becomes the tool of choice to continue their criminal behavior from behind the prison walls.

The High Cost of Inmate Telephone System Security Breaches

Reports of this kind are far too common. In 1999, the Office of the Inspector General in the U.S. Department of Justice released a scathing report on the pervasive nature of inmate telephone system-based crime in federal corrections facilities run by the U.S. Bureau of Prisons. The report focused on a number of criminal investigations involving everything from the crimes described above to conspiracy, firearms, racketeering, fraud, and other crimes.



Inmate Crimes Using the ITS: DOJ Prosecutions Found '85-'98

Drug Conspiracy/Drug-Related	66
Conspiracy	55
Tampering, Threatening &/or Killing Witnesses	30
Wire Fraud	16
Mail Fraud and Theft	15
Racketeering/RICO	15
Murder or Attempted Murder	14
Money Laundering	8
Obstruction of Justice	7
Firearms	5
Smuggling, Theft & Forgery	5

Source: US Department of Justice Survey of US Attorneys' Offices. 1998: 72 responded of 92 offices surveyed.

Breakdown of crimes committed by inmates and prosecuted by the US Department of Justice

Two important points about these figures bear examination. The first is the small number of criminal calls detected and prosecuted in a 13-year period. One might be tempted to look at these figures and conclude that the incidence of inmate telephone system-related crime is relatively tiny compared to the large population of inmates. But a more in-depth analysis would reveal that the small number of prosecutions more closely reflects the primitive nature of the investigative tools at the disposal of corrections investigators. Corrections experts suspect that the number of actual crimes committed is far higher than those reported here. As the old adage goes, "We don't know what we don't know."

The second point to consider about these figures is that a full two thirds of these crimes were found by outside agencies. Thus in two out of every three of these cases, the Bureau of Prisons itself was completely unaware of the crime until notified by an external source. The implications of this report caused major changes in telephone monitoring policy at the Bureau of Prisons.

Despite the recommendations that the Department of Justice made in this report, and the best efforts of the Bureau of Prisons and corrections institutions, it seems the amount of inmate telephone system-related crime has not decreased significantly. News reports of crimes originating from jails and prisons across the country continue to be churned out by the media. The reality is that these kinds of crimes and violations have not only continued, they have increased dramatically.

But how do these crimes happen, when corrections institutions are vigilant in their efforts to stop them? The answer lies in the limitations of the tools these institutions use to prevent the crimes. While a few tools have proven effective, far too often they are no match for resourceful inmates. As we shall see, a few simple strategies used by inmates who want to hide their activities have let inmates undermine the efforts of correctional institutions.

Key Challenges for Today's Inmate Telephone System Security

The current state of the art in inmate telephone system security is multifaceted. These security systems include:

PINs and PANs. Individual inmate phone accounts, and the corresponding Personal Identification Numbers, or PINs (unique strings of digits that the inmates are meant to keep private), are designed to make tracking the phone activities of a given inmate easier and more straightforward. Also in use at some facilities is a strategy known as Personal Allow Numbers, or PANs. A PAN is a list of telephone numbers that an inmate is allowed to call. All other numbers are supposed to be off-limits to the inmate.

Recording of all inmate calls. This practice, begun in the 1990s, has been both a help and a limitation for inmate telephone surveillance. Recording every call means investigators can access and listen to any call made (other than attorney calls) — if they can find the call they seek. A typical 1,000-bed corrections facility generates, on average, 53,000 hours of inmate calls per year. This translates to 26 man-years worth of full-time listening. This "sea" of recorded call data rapidly becomes too large to let corrections departments isolate and review suspicious calls. As a result, this overwhelming call database is a place where inmates can bury any trace of their most "sensitive" calls.

Random inmate call monitoring. The Bureau of Prisons mandates that its corrections institutions monitor at least 10-15% of all inmate calls. This poses significant challenges. For example, unless a human listener is familiar with a given voice, he has a limited ability to pick that voice out of a group of 20 or more candidate voices heard. These limits on human capabilities, together with the sheer call volume required to reach the 15% threshold, make these goals unwieldy for most institutions. Further, the estimated average random monitoring at today's corrections facilities is less than 4% — leaving the other 96% of calls completely unmonitored.

Pre-call validation. This strategy, which generally involves technology known as biometric verification, usually includes one of the following: voice ID, fingerprint verification, or the swiping of an RFID (radio frequency identification) bracelet against a sensor that can verify the ID against the PIN number. Pre-call validation puts a stop to PIN stealing, since the would-be thief lacks the correct voice, bracelet or fingertip when placing the call. However, this technology's utility begins and ends before the call is placed. The inmate who, upon successful verification, willingly hands the phone to another inmate utterly trumps the system and compromises the integrity of that entry in the database.

The ability to search call records on criteria such as phone numbers and PINs has been available since the 1990s and represents basic functionality for investigators. However, a recent study conducted at a large county correctional facility in Florida found that more than 11% of inmate calls involved PIN sharing — corrupting the recorded call database by breaking the relationship between an inmate's PIN and the calls on which his voice appears. This corruption undermines an investigator's ability to search for an inmate by PIN.

All of the security precautions mentioned above thwart some inmates in their attempts to "work the system." However, many inmates are able to get through these barriers.

Why Corrections Facilities Need Better Inmate Telephone System Security Management

Conventional security systems suffer from several limitations:

- They make it difficult for investigators to detect cases of PIN stealing, in which an inmate obtains another inmate's PIN and makes calls on the other inmate's account without the inmate's approval.
- They cannot detect incidents in which one inmate hands the phone to another inmate after validating his identity. This activity is known as PIN sharing.
- They provide no ability to track the true telephone system usage of inmates who employ PIN stealing or PIN sharing.

That said, current biometric verification technologies used in pre-call validation systems do offer a solution to PIN stealing. Since these systems require the owner of the PIN to further identify himself prior to making the call, inmates find it difficult or impossible to steal other inmates' PINs. However, the inmates who want to mask their most important calls from view soon learn that PIN sharing is a way to get around this. Thus, PIN sharing among inmates has become the easiest way for an inmate to mask his identity and criminal intent. The logic behind PIN-sharing is surprisingly straightforward:

- Many inmates are both dishonest and smart.
- Smart inmates exchange PINs on calls they want to hide.
- PIN-shared calls are nearly untraceable by corrections investigators.
- Most inmate telephone systems offer nothing more sophisticated to investigators than the ability to run searches on inmate-entered PINs.
- Investigators thus run PIN-based searches that are doomed to fail.
- Therefore, inmates can conceal their identities on any call they want.

- The recorded call database is thus corrupted, undermining future attempts to build cases against inmates committing crimes using the telephone system.

Given the evidence, we know that a growing number of inmates are conducting criminal behavior over the phones in correctional facilities as if they were not incarcerated at all.

But what if corrections investigators had a tool that accurately determined when an inmate was making a call, whether he used his own PIN or not? What if this tool could listen to every call made by every inmate, and accurately report whenever an inmate's voice appeared on a call that didn't involve his own PIN? What if this same tool could detect every 3-way call bridged by the called party as well as every case of an inmate calling another inmate via a 3-way call?

Voice-Identity-Based Inmate Telephone System Security: A Quantum Leap Ahead

The answer can be found in a little-known area of artificial intelligence research known as continuous-speech voice identification. One of the reasons this field is not well known is because on the surface it sounds a lot like fields to which it is closely related.

For example, the field of speech recognition, which is the ability of a computer to listen to speech and determine the words that were spoken, is used today in products ranging from automatic dictation software to low-cost interactive toys. Speech recognition systems try to answer the question, "Can I understand the word or words you are saying to me?"

The field of biometric verification often includes a kind of technology called voice identification, or simply voice ID. This relies on a system that prompts an individual to repeat one or more specific phrases in turn. The system then compares the speaker's voice to the samples of the same phrase, spoken and recorded by the same speaker at some time in the past. Voice ID says, "Prove to me that you are who you say you are. Let me hear you say a phrase just like you said it before, so I can compare them and be sure." Although not foolproof, voice ID has a degree of accuracy that makes it a suitable choice for inmate pre-call validation systems.

Speech synthesis, also known as text-to-speech or simply TTS, is also in the same general domain. TTS aims to let a computer read text aloud, simply trying to sound as much like a human as possible. When you hear an artificial-sounding voice on a telephone answering system, it is usually a TTS system doing the "speaking."

By contrast, the challenges of continuous-speech voice identification are much greater. Continuous-speech voice identification aims to do something that humans are not very good at: listen to a phone call and try to determine who is doing the talking without the benefit of prompts like those in a voice ID system. In order for a continuous-speech voice identification system to work in a corrections facility, it would have to first learn to recognize the voice of every inmate there. Then it would listen to every call, distinguishing the inmate's voice from that of the called party and from line or background noise. Ideally, it would be able to tell if more than one inmate were on the call, pick out both voices, and match those voices to the ones it had memorized.

The Value of Voice-Based Inmate Telephone System Security Management

A continuous-speech voice identification system adapted for use in monitoring inmate telephone systems has high value for corrections institutions. Such a system would rely on the voice of the speaker for identification and in call monitoring. In fact, the right set of voice-based tools would give corrections facilities the ability to do the following:

- Track illicit phone activities as they occur.
- Decide if, when, where and how to intervene in these activities.
- Find all calls on which a given inmate's voice appears, whether or not the inmate placed the call using his own PIN.
- Understand exactly how much abuse of the system occurs, and when it occurs.
- Furnish complete information to external agencies and prosecutors when requested.
- Crack difficult investigations on targeted inmates.
- Detect and prevent crime originating from inside the walls of corrections facilities.

Investigator Pro™ Inmate Telephone System Crime Detection & Prevention System

JLG Technologies' Investigator Pro is a software system based on continuous-speech voice identification and is designed specifically for corrections investigators. Investigator Pro analyzes calling patterns to tell investigators and administrators which calls are high risk, which inmates are violating facility rules, and how to uncover the tracks that inmates know how to hide from corrections officials. Moreover, Investigator Pro analyzes all inmate calls and looks for risky or suspicious patterns of phone use. It flags PIN abuse calls, 3-way calls, and calls made from one inmate to another, both within an agency and between agencies across the country. It gives investigators the tools to track suspicious calling activity by individual voices, not just by PIN or telephone number, and to uncover criminal associations and activities.

Investigator Pro enables corrections institutions to take control of phone-related inmate crimes and rule violations that go undetected by conventional monitoring technology. Investigator Pro is a set of powerful investigative tools designed specifically for corrections investigators.

An Overview of Investigator Pro Modules

Below is a brief summary of Investigator Pro's major components:

QuickFind™ uncovers patterns of suspicious behavior and shows them to the investigator. The investigator can drill down with a single touch on any item — revealing, for example, all calls made by a given inmate to a specific number, the names of any other inmates who called that same number, or calls made by other inmates using the given inmate's PIN. All such calls are displayed, complete with clear markers that flag calls with suspicious elements such as 3-way call events or multiple inmates on the call. QuickFind also presents a list of recent high-target calls for the investigator to review, cutting down on the time he needs to spend listening to calls in search of leads.

VoiceSearch™ allows investigators to find all calls on which an inmate's voice appears. Investigators can then filter them, for example, showing only those calls in which the inmate's voice appears but another inmate's PIN was used to place the call. Investigators can also search on a called party's voice and identify all the calls on which that voice appears.

CallPlayer Pro™ lets corrections investigators play, visualize and annotate inmate calls. They can play the inmate and called party sides of the call separately or together, and speed up or slow down playback to improve intelligibility. An investigator can capture and save a voice clip from either the inmate or called party side and use that clip to search the database for all calls where that voice occurs.

Suspicious CallFinder™ automatically generates leads by finding calls that match a wide array of criteria associated with suspicious behavior including PIN theft, PIN sharing, and 3-way calls.

CallFinder™ provides search capabilities by inmate PIN or a host of other criteria. Calls retrieved may be filtered and sorted by one or more criteria out of a large number of call information details.

MyCallReview™ presents a corrections investigator with a list of calls he has already listened to, and enables him to sort his calls by case, inmate, telephone number, PIN, or other criteria.

ReportMaker™ collects and organizes findings into cohesive reports, often revealing difficult-to-spot patterns of criminal behavior for the first time.

Settings lets the facility define its own user roles with different system privileges. It includes an easy way for the facility to create custom high-interest group categories, such as particular gangs, for inmates and called party telephone numbers.

How Investigator Pro Adds Value for Corrections Institutions

The ability to identify and monitor incidences of PIN sharing, PIN stealing, multiple inmates on a call and 3-way calls directly benefits the corrections institution. Having investigative tools based on inmate voices, rather than just on PINs, means that investigators no longer need to rely on the honesty, integrity or ignorance of convicted criminals to conduct effective investigations. Investigator Pro analyzes every minute of every call. Further, calls are monitored by a system that learns the voice of every inmate — and never forgets it. Better call surveillance means more effective management of security at correctional facilities, which is good news not just for the facilities, but for investigators, managers, officers, and the public at large.

But according to investigators at facilities where Investigator Pro is already hard at work, there are other benefits as well. Investigator Pro streamlines the workflow for investigators. Its advanced design enables corrections investigators to spend less time sifting through irrelevant call data, and more time gathering the critical pieces of their investigations and connecting them together. In addition, less inmate conflict means more peaceful day-to-day life. When inmates have their calling card hours stolen, or are coerced into giving their PINs to other inmates, they have little recourse but to complain to the facility's officers. By reducing inmate-to-inmate crime, Investigator Pro helps keep inmates more content — reducing incidental costs in the process.

JLG Technologies' Vision for the Future of Inmate Telephone System Security

JLG Technologies is committed to maintaining the leading edge of voice-based security management solutions. With multiple patents filed and more on the way, JLG Technologies will continue to innovate to make sure the balance of power in inmate telephone system abuse stays on the side of the corrections facilities. To find out more about JLG Technologies, visit www. JLGTechnologies.com.

About JLG Technologies

JLG Technologies (www.JLGTechnologies.com) is the leader in voice biometric software for investigators in the corrections and law enforcement industry. Its software products use state-of-the-art voice identification technology to pinpoint suspicious telephone activity and help investigators uncover and prevent crime. JLG Technologies is a privately held company with its headquarters in Framingham, Massachusetts.