Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege

Jordan Smith, Micah Lee – The Intercept

https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/

Nov. 11 2015, 5:43 p.m.

AN ENORMOUS CACHE of phone records obtained by *The Intercept* reveals a major breach of security at Securus Technologies, a leading provider of phone services inside the nation's prisons and jails. The materials — leaked via SecureDrop by an anonymous hacker who believes that Securus is violating the constitutional rights of inmates — comprise over 70 million records of phone calls, placed by prisoners to at least 37 states, in addition to links to downloadable recordings of the calls. The calls span a nearly two-and-a-half year period, beginning in December 2011 and ending in the spring of 2014.

Particularly notable within the vast trove of phone records are what appear to be at least 14,000 recorded conversations between inmates and attorneys, a strong indication that at least some of the recordings are likely confidential and privileged legal communications — calls that never should have been recorded in the first place. The recording of legally protected attorney-client communications — and the storage of those recordings — potentially offends constitutional protections, including the right to effective assistance of counsel and of access to the courts.

"This may be the most massive breach of the attorney-client privilege in modern U.S. history, and that's certainly something to be concerned about," said David Fathi, director of the ACLU's National Prison Project. "A lot of prisoner rights are limited because of their conviction and incarceration, but their protection by the attorney-client privilege is not."

The blanket recording of detainee phone calls is a fairly recent phenomenon, the official purpose of which is to protect individuals both inside and outside the nation's prisons and jails. The Securus hack offers a rare look at this little-considered form of mass surveillance of people behind bars — and of their loved ones on the outside — raising questions about its scope and practicality, as well as its dangers.

Securus markets itself to government clients as able to provide a superior phone system — its Secure Call Platform — that allows for broad monitoring and recording of calls. The company also promotes its ability to securely store those recordings, making them accessible only to authorized users within the criminal justice system. Thus, part of the Securus promise is not only that its database is vast, but also that it meets rigorous standards for security. "We will provide the most technologically advanced audio and video communications platform to allow calls with a high level of security," reads the company's Integrity Pledge. "We understand that confidentiality of calls is critical, and we will follow all Federal, State, and Local laws in the conduct of our business."

But the fact that a hacker was able to obtain access to over 70 million prisoner phone call records shows that Securus' data storage system is far more vulnerable than it purports to be.

More broadly, the Securus leak reveals just how much personal information the company retains about prisoners and the countless people to whom they are connected. It is information that, in the narrow context of incarceration, may not be considered private, but in the larger world raises serious questions about the extent to which people lose their civil liberties when their lives intersect, however briefly, with the criminal justice system.

* * *

SECURUS IS A TELECOMMUNICATIONS company based in Dallas, Texas, owned by a private equity firm. Its primary business is providing phone and video visitation services to incarcerated people — ostensibly offering a meaningful way for them to keep in touch with loved ones on the outside, as well as to communicate with attorneys. Until now, Securus was probably best-known for the incredibly high rates it has traditionally charged for phone calls, a burden borne almost exclusively by the very people who are the least able to afford it. (The Federal Communications Commission in October voted to cap calling rates and fees, a move that Securus and other industry leaders had fought, claiming the change would have a "devastating effect" on their businesses.)

It isn't just Securus whose business model has relied on gouging people caught up in the criminal justice system. The industry's other players, including the leading prison telecom company, Global Tel*Link, largely do the same. Prison and jail communications is a $1.2 billion a year business, whose handsome profits come from serving a captive and inelastic market. According to public relations materials, Securus provides communications platforms used by more than 1.2 million inmates across the country, who are confined in more than 2,200 facilities; by 2012 the company was processing more than 1 million calls each day. In 2014, Securus took in more than $404 million in revenue.

Securus does business with local and county governments (which operate the nation's jails) and with state departments of correction (which, with some exceptions, run the nation's prison systems). A key selling point to its clients is that the company not only installs and maintains phone systems at little to no cost to the government, but also that it agrees to pay back to its clients generous "site commissions," a kickback that comes from revenue generated by inmate calls — on average 42 percent of the revenue from its state contracts, according to research done by *Prison Legal News*. (The FCC rate caps threaten the industry's ability to keep revenues large enough to fund the exorbitant kickback scheme it created. Lowering and capping the rates and fees charged for calls means at least some industry players could be forced to dip into company coffers in order to comply with contracted payoff schedules, unless they renegotiate existing contracts. How the new rate caps will impact these payoffs remains to be seen.)

> "OMG ... this is not good!" reads an internal Securus email discussing phone calls hacked in 2014.

In addition to the sweetheart deal it offers clients, Securus also touts the technology of its Secure Call Platform, which allows recording and monitoring, with few exceptions, of all calls made by prisoners. The superior technology, it claims, ensures that its database is well-protected, and only accessible to authorized users — among them corrections workers, police investigators, and prosecutors. Law enforcement personnel are particularly important to the company: Securus promises it can provide recordings on demand to investigators across jurisdictions, promoting its system as a powerful crime-solving tool.

But the scale of the Securus hack shows the company has failed to fulfill its own promises on security. The more than 70 million phone call records given to *The Intercept* include phone calls placed to nearly 1.3 million unique phone numbers by more than 63,000 inmates. The original data was contained in a 37-gigabyte file and scattered across hundreds of tables, similar to spreadsheets, which *The Intercept* merged into a single table containing 144 million records. A search for duplicates reduced this figure to more than 70 million records of individual phone calls.

The database contained prisoners' first and last names; the phone numbers they called; the date, time, and duration of the calls; the inmates' Securus account numbers; as well as other information. In addition to metadata, each phone call record includes a "recording URL" where the audio recordings of the calls can be downloaded.

The vast majority of the calls appear to be personal in nature; downloaded audio files leaked alongside the larger database of recordings include one in which a couple has an intimate conversation; in another, relatives discuss someone whose diabetes is worsening. In a third, a couple discusses *Dancing With the Stars*, TV dinners, and how much money is available to pay for their regular phone conversations — versus how much should instead be spent on food. But a subset of the recordings — a minimum of roughly 14,000 — were made by detainees to attorneys, in calls that range from under a minute to over an hour in length.

To arrive at this figure, *The Intercept* looked up each of the nearly 1.3 million phone numbers that inmates called in a public directory of businesses to find out whether a law firm or attorney's office is associated with that number. We found that Securus recorded more than 14,000 phone calls to at least 800 numbers that clearly belonged to attorneys. That 14,000 figure, however, is likely an underestimate because it does not include calls to attorney cellphone numbers. In other words, the 14,000 attorney calls are potentially just a small subset of the attorney-client calls that were hacked.

In short, it turns out that Securus isn't so secure.

In fact, this doesn't seem to be the first time that Securus' supposedly impenetrable system has been hacked. According to documents provided to *The Intercept* by a Texas attorney, the company's system was apparently breached just last year, on July 18, 2014, when someone hacked three calls made by an inmate named Aaron Hernandez, presumably the former player for the New England Patriots, who was awaiting trial for killing a friend. In an email thread from July 21, 2014, two Securus employees discuss the breach — the system was accessed by someone in South Dakota, they discover, though they don't have that person's name. "OMG.....this is not good!" reads one email contained in the document. "The company will be called to task for this if someone got in there that shouldn't have been."

There is no indication the 2014 hack has previously been made public. Securus did not respond to numerous requests for comment for this story. [*Editor's note: See update below for a statement from Securus in response to publication of this story.*]

* * *

PRISONERS DO NOT GENERALLY ENJOY a right to privacy while incarcerated — a fact that is emphasized in the course of virtually any communication with the outside world. Like other jail and prison telecoms, Securus inserts a recorded message at the beginning of each prisoner-initiated phone call, reminding recipients that "this call is from a correctional facility and may be monitored and recorded." In this context, anyone who hears the warning and still chooses

to use the phone has effectively waived a right to privacy during that call, a condition all too familiar to people with incarcerated loved ones. Still, it is hard to imagine that people on either end of the line would ever anticipate that their conversations would be stored for years, in a manner that could potentially expose their intimacies to the larger public. By failing to prevent hackers from accessing the calls, Securus appears to have done just that.

This is troubling to the ACLU's Fathi, because "waivers of rights are not meant to be all or nothing. Waivers are meant to be only as extensive as necessary to accomplish the goal underlying the waiver," he said. If the goal for recording and monitoring detainee phone conversations is to enhance safety both inside and outside a facility that's one thing — but those conversations should not be stored indefinitely, once they're determined to be free of intelligence that would aide the institutional goal.

The mass recording of detainee calls was originally rationalized as improving safety within a facility — a way to hedge against contraband being brought in, to ferret out escape attempts or potentially violent uprisings, and to curb the possibility of witness tampering or intimidation. But if the goal is to see if a "person is smuggling drugs [or] plotting an escape," said Fathi, "it doesn't mean that the prisoner and the ... outside person they're talking to has forever waived all privacy rights and that any conceivable use of that recording is OK."

The implications are especially alarming for calls that are understood to be the exception to the record-everything rule. Securus' phone systems are supposed to be set up to allow certain phone numbers to be logged and flagged so that calls to those numbers are exempt from being recorded — let alone stored.

Indeed, that a criminal defendant or inmate should be able to speak frankly and honestly with a lawyer is a cornerstone of the criminal justice system — inherent in a defense attorney's ethical obligations, and firmly rooted in the Sixth Amendment right to competent and effective legal counsel. A review of contracts and proposals completed by Securus in a handful of states reflects the company's understanding of this right. In a 2011 bid to provide phone service to inmates in Missouri's state prisons, Securus promised that each "call will be recorded and monitored, with the exception of privileged calls." But the database provided to *The Intercept* shows that over 12,000 recordings of inmate-attorney communications, placed to attorneys in Missouri, were collected, stored, and ultimately hacked.

The data provided to *The Intercept* also includes at least 27 recordings of calls to attorneys in Austin, Texas, made between December 2011 and October 2013 — a fact that is particularly compelling in light of a federal civil rights suit filed there in 2014 against Securus, which provides phone service to the county's jails. At the heart of the lawsuit is the allegation that calls to known attorneys have been — and continue to be — recorded. The company's contract specifically provides that calls "to telephone numbers known to belong [to] attorneys are NOT recorded" and that "if any call to an attorney is inadvertently recorded, the recording is destroyed as soon as it is discovered."

The lawsuit was brought by the Austin Lawyers Guild, four named attorneys, and a prisoner advocacy group, and alleges that, despite official assurances to the contrary, privileged communications between lawyers and clients housed in the county jails have been taped, stored, "procured," and listened to by prosecutors. The plaintiffs say that while some prosecutors have disclosed copies of recordings to defense attorneys as part of the regular evidential discovery process, other prosecutors have not, choosing instead to use their knowledge of what is in individual recordings to their "tactical advantage" in the courtroom

"without admitting they obtained or listened to the recordings." (None of the recordings provided to *The Intercept* appear to be connected to any of the Austin attorneys named in the suit.)

The Austin attorneys argue that the intrusion into their communications with clients undermines their ability to effectively represent them. And those most disproportionately impacted are often clients who are the most disadvantaged: those who can't afford bail and have to stay in jail awaiting prosecution. Austin defense attorney Scott Smith, who discovered this summer that an intern in the prosecutor's office had inadvertently listened to a portion of a phone call he had with a jailed client, points out that it rigs the adversarial legal process in favor of the state. "How do you plan your strategy? It's like being at the Superbowl and one team gets to put a microphone in the huddle of another team."

Challenging the lawsuit, Securus notes that government intrusion into the attorney-client relationship could be a violation of the Sixth Amendment. But the company insists it has abided by its policy of not recording privileged phone calls — while at the same time maintaining that any existing tapes were voluntarily turned over by the state to defense attorneys during discovery. What's more, Securus argues that the plaintiffs have not proved that "such recordings" had any adverse effects on their cases. "Securus acknowledges that Plaintiffs have alleged that recorded attorney-client calls have been shared with prosecutors, but they have failed to articulate a single instance where they have been harmed or prejudiced," Securus said.

Exactly who is to blame for the recording of attorney calls is unclear. In many jurisdictions — including in Austin — the onus is on lawyers or their clients to give phone numbers to prison officials so that they can be placed on a do-not-record list. Failing to provide up-to-date contact information would make any inadvertent recordings the attorney's or inmate's fault. But properly logging these numbers is the government's responsibility. And the secure storage of these is squarely up to Securus — particularly given that it markets itself as providing a service to do exactly that.

* * *

IT WASN'T ALWAYS THE CASE that detainee phone calls were recorded in bulk. The practice really took hold in the 1990s, says Martin Horn, a lecturer at John Jay College of Criminal Justice in New York, who previously served as commissioner of the New York City Department of Correction and, before that, as secretary of corrections in Pennsylvania. When Horn went to Pennsylvania in 1995, the state did not allow for the recording of inmate calls. But that decade saw "numerous horror stories," he said, of inmates "perpetrating crimes" from within prison, "continuing to run their criminal enterprises" from behind bars, or "threatening witnesses, and so on." At the same time, telephone technology had evolved significantly, making monitoring, recording, and storage of call data possible.

Until the mid-1980s, inmate phone services were provided by AT&T via operator-assisted collect calls from pay phones. But after the breakup of AT&T the market became more competitive — and less regulated — and companies such as Securus, originally known as the Tele-Matic Corporation, entered the market to offer equipment and, ultimately, sophisticated monitoring systems.

Today, Horn regards call monitoring as an important correctional tool. And while Horn said he was never made aware of any recording of attorney-client communications during his time in corrections, he said to the extent that a privileged communication is either monitored or recorded, there isn't necessarily a harm — "if in the course of listening to it you become aware

that it's a conversation with a privileged party, such as an attorney, you stop listening," he said. "So the fact that it was recorded, while unfortunate, you know, isn't necessarily damaging."

> The hacked database also includes records of calls between prisoners and prosecutors — including 75 calls to a U.S. attorney's office in Missouri.

But the massive amount of data provided to *The Intercept* suggests that the scope of surveillance within the system goes far beyond what the original goals might have been. A 2012 Securus contract with the Illinois Department of Corrections describes an optional product called Threads, branding it "one of the most powerful tools in the intelligence community."

"Securus has the most widely used platform in the industry, with approximately 1,700 facilities installed, over 850,000 inmates served, literally petabytes of intelligence data, and over 1 million calls processed per day," the company bragged to Illinois officials. "This valuable data is integrated directly into Threads and could be available at [Department of Correction]'s and [Department of Juvenile Justice]'s fingertips."

Today those numbers are even higher. Securus' website says that the Threads database contains the billing names and addresses of over half a million people who are not incarcerated, as well as information about more than 950,000 inmates from over 1,900 correctional facilities, and includes over 100 million call records. The amount of data sold to corrections and law enforcement investigators "continues to grow every day."

As Adina Schwartz, a professor at John Jay College, points out, when you consider that these recordings can be stored "forever, with no supervision," the potential for abuse increases. "I think any criminal defense attorney who wasn't worried by that prospect is basically somebody who doesn't do his or her job."

And the recordings with known attorneys are not limited to calls with defense lawyers. The hacked database also includes records of calls between prisoners and prosecutors — including 75 calls to a United States attorney's office in Missouri. These, too, are potentially problematic, particularly if they include conversations with cooperating witnesses who could be vulnerable if the details of their dealings with the government were exposed.

The attorney-client privilege is "the oldest privilege of confidentiality known in our legal system," said Fathi. In a criminal case it prohibits defense attorneys from divulging, or prosecutors from using, any case-related information that was obtained in confidence. But the reality is that keeping conversations with incarcerated defendants confidential is a challenge. Experts point out that the recorded notice embedded within phone calls initiated inside jails and prisons means that there should be no real expectation of privacy. "If a client is making an out-of-prison call to an attorney, the attorney-client privilege, arguably, doesn't apply," said Michael Cassidy, a professor of law at Boston College Law School, because by consenting to speak over a phone line that is subject to recording, the client and attorney should expect that is happening. But that isn't the end of it: Even if the privilege doesn't apply, "the Sixth Amendment right to counsel applies and the government can't interfere with it," he said. "So even if you could argue that notifying a prisoner that their calls are being recorded negates the privilege, it doesn't negate the Sixth Amendment right to not have the government interfere with counsel." And monitoring, recording, and potentially using information gleaned from attorney-client calls would do just that.

That's why prison calling systems, such as Securus' Secure Call Platform, are set up to log numbers that should not be recorded. "But that's a technological issue and sometimes it doesn't work," said Cassidy.

But Schwartz argues that the logging of attorney phone numbers provides a "recognition that there is attorney-client privilege" and that it is "incumbent on the government to follow through" in protecting that privilege. When attorneys learn that their calls have been recorded, it shakes the foundation of trust, inevitably impinging on their Sixth Amendment obligations. "Once people know there is trickery, there is a chilling of attorney-client communications — because how do you know it won't happen again?" Schwartz asked.

Indeed, that is precisely the risk that Fathi sees arising from the breach of Securus' database. "Going forward, prisoners will have very good cause to question whether their phone calls with their attorneys are confidential. And that undermines that very core and fundamental purpose of the attorney-client privilege, which is to allow persons consulting an attorney to give a full and frank account of their legal problem," he said.

Still, challenging the recording could be tricky, says Cassidy, even if there is clear evidence of taped communications. If a call was recorded because the attorney or client failed to put a phone number on the do-not-record list, he says, then the state is off the hook — a prisoner can't sue for damages, or seek to have his or her criminal charges dismissed (although the government would still be prohibited from listening to or using the content of the call). However, if one can "show a regular and systemic practice" of recording such calls, a case could be made that "the company is violating multiple prisoners' Sixth Amendment rights," which could have more of an impact, perhaps prompting systemwide reforms.

And Fathi believes a case could also be made that the recording and storing of non-attorney calls is unconstitutional. "Prisoners do retain some privacy rights and certainly people on the outside who just happen to be talking to prisoners retain privacy rights. And, again, the fact that you're passively consenting that the call can be monitored for security purposes doesn't mean you're consenting to all conceivable uses of that recording for all time," he said. "I think even with the non-attorney calls there may be a case to be made that this is just so spectacularly overbroad that it is unconstitutional."

Indeed, Austin attorney Scott Smith believes that, at least in the nation's jails — where the majority of inmates are awaiting prosecution and have not yet been found guilty of anything — the blanket recording of phone calls should be stopped. If there are specific detainees worth monitoring, that can be accomplished in a far less intrusive manner, he said. "You can say safety mandates a reduction of civil liberties all the time. And that's essentially the old debate — how much do you have civil liberties and how much do you need to get rid of them in order to be safe?"

Fathi agrees that the practice of recording detainee phone conversations should be reined in and limited. "It is another manifestation of the exponential growth of the surveillance state. Obviously that's been noticed and commented upon in other contexts, but if we're talking about [more than 70] million [calls], even if some of those are repeat calls between the same people, that's a lot of people — including non-prisoners whose privacy has been compromised by a private company that is acting as an agent of the government," he said.

Update: November 12, 2015

After this story was published, Securus emailed the following statement:

> Securus is contacting law enforcement agencies in the investigation into media reports that inmate call records were leaked online. Although this investigation is ongoing, we have seen no evidence that records were shared as a result of a technology breach or hack into our systems. Instead, at this preliminary stage, evidence suggests that an individual or individuals with authorized access to a limited set of records may have used that access to inappropriately share those records.
>
> We will fully support law enforcement in prosecution of any individuals found to have illegally shared information in this case. Data security is critically important to the law enforcement and criminal justice organizations that we serve, and we implement extensive measures to help ensure that all data is protected from both digital and physical breaches.
>
> It is very important to note that we have found absolutely no evidence of attorney-client calls that were recorded without the knowledge and consent of those parties. Our calling systems include multiple safeguards to prevent this from occurring. Attorneys are able to register their numbers to exempt them from the recording that is standard for other inmate calls. Those attorneys who did not register their numbers would also hear a warning about recording prior to the beginning of each call, requiring active acceptance.
>
> We are coordinating with law enforcement and we will provide updates as this investigation progresses.

Research: Margot Williams, Joshua Thayer

Contact the authors:

Jordan Smith✉jordan.smith@theintercept.com

Micah Lee✉micah.lee@theintercept.com