Lawyers Speak Out About Massive Hack of Prisoners' Phone Records

Jordan Smith, Micah Lee – The Intercept

https://theintercept.com/2016/02/12/not-so-securus-lawyers-speak-out-about-massive-hack-of-prisoners-phone-records/

Feb. 12 2016, 5:49 p.m.

IN THE SUMMER of 2013, Missouri criminal defense attorney Jennifer Bukowsky was preparing for an evidentiary hearing in the case of a pro bono client, Jessie McKim. The stakes were high: Along with his co-defendant, James Peavler, McKim had been convicted in 1999 of killing a woman named Wendy Wagnon and was serving life without parole at a maximum security prison. At the upcoming hearing, Bukowsky planned to argue that her client was innocent — and that the murder that sent him to die in prison was never a murder at all.

McKim was convicted in part based on the testimony of a local medical examiner, who claimed that the presence of petechiae on a dead body — small spots on the skin or the whites of the eyes where capillaries have hemorrhaged — is proof that a person was suffocated. But a toxicology report — completed after Wagnon's cause of death had already been determined as asphyxiation — revealed that Wagnon had lethal levels of methamphetamine in her system when she died. Among the witnesses Bukowsky planned to call at the hearing were five different pathologists who would testify that the state's medical examiner was wrong when he claimed Wagnon was suffocated — and that evidence pointed to a meth overdose instead. (A sixth pathologist, retained as an expert by the state, also agreed that Wagnon died of an overdose, not of suffocation.)

"It was a really big time, and a crucial time, for his case," Bukowsky recalls. As she prepped witnesses and decided who else should take the stand, she shared her strategy with McKim via lengthy phone calls — calls understood to be protected by attorney-client privilege. Unlike calls between prisoners and their family or acquaintances, which are routinely monitored, conversations with lawyers are not to be recorded. During these calls, says Bukowsky, "I'm telling him my concerns about calling this or that person — that is crucial information that should be private between us."

The hearing took place in August 2013. The following spring, a circuit court judge ruled against McKim, upholding his conviction and saying that even if Wagnon was not suffocated, McKim and his co-defendant could have killed her another way — by intentionally forcing her to overdose on meth, a theory the state had never previously argued, for which there was no supporting evidence.

Bukowsky was confounded by the ruling, but remained undeterred — she is convinced of McKim's innocence and knows from experience that in a system that favors finality, undoing an unjust conviction can be frustrating work. "It takes a lot of grit & it makes me angry," she wrote in an email.

Last fall, Bukowsky received an unexpected phone call related to McKim's case. The call came from *The Intercept*, following our November 11, 2015, report on a massive hack of Securus Technologies, a Texas-based prison telecommunications company that does business with the Missouri Department of Corrections. As we reported at the time, *The Intercept* received a massive database of more than 70 million call records belonging to Securus and coming from prison facilities that used the company's so-called Secure Call Platform. Leaked via SecureDrop

by a hacker who was concerned that Securus might be violating prisoners' rights, the call records span a 2 1/2-year period beginning in late 2011 (the year Securus won its contract with the Missouri DOC) and ending in the spring of 2014.

Although Securus did not respond to repeated requests for comment for our November report, the company released a statement condemning the hack shortly after the story was published. Securus insisted there was "absolutely no evidence" that any attorney-client calls had been recorded "without the knowledge and consent" of the parties to each call.

The Intercept's analysis, to the contrary, estimated that the hacked data included at least 14,000 records of conversations between inmates and attorneys. In the wake of the story's publication, we informed Bukowsky that her phone number had been found among the records and provided her a spreadsheet of the calls made to her office — including the name of the client and the date, time, and duration of the calls. In turn, Bukowsky searched her case files for notes and other records, ultimately confirming that at least one call with McKim — which was prearranged with the Missouri DOC to be a private attorney call — was included in the data. The privileged call, more than 30 minutes long, was made at the height of Bukowsky's preparations for McKim's hearing. A unique recording URL accompanied each of Bukowsky's calls included in the data, suggesting that audio had been recorded and stored for more than two years — and ultimately compromised by the unprecedented data breach.

The discovery was distressing. "I was in the thrust of litigating with the state attorney general's office a very hotly disputed habeas petition, and I was acting under good faith that they were not recording," she said. "And," it appears, "they were."

* * *

THE ABILITY OF COUNSEL and client to communicate confidentially is a cornerstone of the American legal system. The recording, monitoring, or storage of such legally protected communications not only chills the attorney-client relationship, but may also run afoul of constitutional protections — including the right to effective assistance of counsel and access to the courts.

The mass recording of inmate calls is itself a fairly recent practice, sold by private telecommunications companies, like Securus, to jails and prisons as a security measure — a way to thwart violent uprisings, for example, or curb the introduction of contraband into a facility. This bulk surveillance — the recording and long-term storage of millions and millions of routine communications — raises serious concerns about the privacy rights of incarcerated persons and their loved ones, says David Fathi, director of the ACLU's National Prison Project. And indeed, while incarceration may compromise some individual rights, a detainee's right to confidential communication with an attorney is not one that can be trampled by the state — or a private company. In criminal cases, the attorney-client privilege bars defense attorneys from disclosing, or prosecutors from using, any case-related information obtained in confidence. It is, says Fathi, "the oldest privilege of confidentiality known in our legal system."

After *The Intercept* exposed the Securus hack, numerous defense attorneys contacted us to find out whether the database contained any of their call data. As we previously reported, the data contained 1.3 million unique telephone numbers; to determine if the 70 million call records contained attorney-client calls, we did a reverse lookup of each number, finding that at least 14,000 calls were made to attorneys. But because the reverse lookup was limited to a commercial directory, and because we searched only for business listings that included the

words “attorney,” “law,” or “legal,” we concluded that we were likely missing thousands of additional calls — including those made to attorney cellphone numbers, which would not necessarily be listed in a commercial directory.

The attorneys who contacted *The Intercept* helped advance our investigation into the data by identifying additional phone numbers as belonging to lawyers, which were not previously included in our estimate. We have now identified at least 43,000 additional records of attorney-client communications — including both attempted and completed calls — contained within the hacked data. (But again, because the subsequent searches were done only for attorneys who reached out to *The Intercept*, we suspect there are still many more attorney-client call records not yet identified in the data.)

Among these additional records are more than 33,000 calls that detainees placed to lawyers working for Missouri’s state public defender office, and more than 1,000 made to the Midwest Innocence Project, which handles wrongful conviction cases in Missouri and four other states. That the hack contained so many calls to the MIP is distressing to the nonprofit’s executive director, Oliver Burnette. “It really gave us pause, and I think it can really hinder how we try to do business for the most vulnerable among us, those people ... who are in jail and may be innocent,” he said.

As with Bukowsky’s calls, some of these additional records correspond to phone conversations arranged with prison officials to be confidential attorney-client communications, which never should have been recorded.

After a detailed review of several specific fields contained within the hacked records, *The Intercept* has been able to narrow the geographical scope of the recorded calls, tracing all of the detainee call records to Missouri prison facilities. Although, as we previously reported, the database reflects calls to at least 37 states, the vast majority — 85 percent — were made to phone numbers in Missouri. An additional 5 percent were placed to numbers with Kansas and Illinois area codes — states that border Missouri’s largest cities, Kansas City and St. Louis. Each phone record includes the name of the prisoner making the call, an acronym for a location that maps to a correctional facility in Missouri, as well as an identification number that appears to correspond with Missouri DOC prisoner IDs. The records do not include the number from which each phone call originated.

For Bukowsky — who founded her eponymous firm in Columbia in 2010 — the potential for damage was vast. At the August 2013 hearing in McKim’s case, the state called to the stand a woman, Melissa McFarland, who was with Wagnon just before her death and then implicated McKim in that death, a circumstance Bukowsky would have discussed with McKim. “So for them to hear me — if they’re listening to me, which I don’t know if they did — but were they to, they would know all the different things that I’m saying to my client that I think are problems for McFarland that I’m going to cross-examine her on [and] they could then prep her accordingly.”

In an email response to *The Intercept*, a spokesperson for the Missouri attorney general said that its office did not have access or listen to any phone calls between Bukowsky and McKim.

Bukowsky notes that violating attorney-client confidentiality in the manner that appears to have happened — and could still be happening, whether in Missouri or any of the jurisdictions where Securus operates, which include 47 states and the District of Columbia, as well as Canada and Mexico — is just another way the odds are stacked in favor of the state in criminal prosecutions.

* * *

IN OUR INITIAL REPORT, the ACLU's Fathi described the hack as potentially representing the "most massive breach of the attorney-client privilege in modern U.S. history." Upon learning *The Intercept* was able to confirm that the data included prearranged, privileged communications between lawyers and their clients, Fathi was even more troubled: "It's very disturbing that calls that were explicitly set up as attorney-client calls were also recorded," he said. "There's no excuse for recording attorney-client calls, and there's certainly no excuse for indefinitely retaining those recordings."

Securus' first public statement following our November report characterized the breach as an inside leak. In a subsequent press release on November 13, the company dropped the language about the hack being an inside job, declaring that it was "working on multiple fronts to fully investigate ... and to prevent future criminal attacks." The company said it had hired a forensic data analysis firm to determine how the hack happened and "to confirm that it happened outside of the Securus network and systems." Securus has not publicly released any additional information related to the breach, nor responded to our requests for additional information and comment for this story.

Securus previously contested *The Intercept*'s conclusions about the recording of potentially privileged calls. "While *The Intercept* reports that they matched call data from the stolen data with phone numbers attached to attorneys' offices," it said in its second release regarding the hack, "no evidence has been provided that any of these calls were actually recorded, and if so, whether any of them would actually constitute privileged communications," In addition, Securus said that its calling systems contain "multiple safeguards to prevent attorney-client recordings from occurring," and pointed out that "licensed attorneys are able to register their numbers or a specific call to exempt them from recording."

Although specific procedures differ depending on the state or locality involved, it is commonly the responsibility of lawyers to verify and register their numbers with jail or prison officials — ostensibly to ensure that legal calls are not recorded or monitored.

"While it is possible that not all of these safeguards were followed by the callers in some cases," the company continued, "we have seen no evidence to date of recorded calls that would fall under that category."

But criminal defense lawyers in Missouri told *The Intercept* that, unlike other jurisdictions in which Securus provides inmate calling services, the Missouri DOC does not allow attorneys to provide individual phone numbers to the agency or to individual facilities for inclusion in a standing do-not-record list. In an email, Missouri DOC Communications Director David Owen said the DOC "respects the right of offenders to have privileged communications with their attorneys" and explained that in order to guarantee a call is private, "attorneys must demonstrate, in written form, they are a licensed attorney, and request to have a privileged telephone call with an incarcerated offender." Once scheduled, such calls are "set to private," he explained, adding that lawyers "must make this request every time they wish to have a privileged telephone conversation with an incarcerated offender."

But, after reviewing call record information provided by *The Intercept*, five attorneys in Missouri confirmed that contained in the hacked data were calls that were prearranged with the DOC to be private communications. "How can a client feel safe sharing information with his attorney when he suspects that the opposing party is listening to the call? How can an attorney expect to share legal strategy with their client if she suspects the same?" asks Jennifer

Merrigan, a defense attorney who has represented Missouri death row prisoners for more than a decade, including as a former staff attorney and director of the Death Penalty Litigation Clinic in Kansas City. "A critical foundation of trust and confidence in the process has been destroyed."

"It's a little bit disconcerting," says Missouri criminal defense attorney Kent Gipson, who discovered three calls made to him by three different clients that he could confirm were set up in advance, through prison authorities, as privileged calls that were not to be recorded. Each call record he identified also contained a unique recording URL. At the same time, Gipson notes, the allegation that all calls, including attorney calls, are routinely recorded or monitored is not a new one among attorneys or inmates. "Nothing much surprises me anymore," he said.

* * *

AFTER REVIEWING RECORDS found in the hacked data for calls made to public defender offices across Missouri, Michael Barrett, director of the Missouri State Public Defender System, said in an email that his office's "initial finding" did not reveal any call records that match up with calls known to have been prearranged by system attorneys. "Not to say it didn't happen," he wrote, "just that we cannot identify a prearranged call that was recorded."

But Barrett is among those *The Intercept* interviewed who suggest that the recording of any attorney-client communications can hinder the effectiveness of counsel. "Confidentiality is at the heart of what we do, and if a client feels as if what they say is being compromised, to whatever degree, he or she may not be sufficiently forthcoming with counsel so that the most effective defense can be presented on their behalf," Barrett wrote. The best approach, he suggests, is to have a policy of never recording phone calls between lawyers and their clients. This would also mean "the risk of confidential information being leaked is zero."

The MIP's Burnette agrees, noting that there is no reason for clients to call except to talk about their cases — and any call in which representation is discussed should be considered privileged and thus not recorded, monitored, logged, or stored. "I think that any time someone calls our office, it's a legal call," he says. "I mean, we're not talking about the [Kansas City] Chiefs game." That is "not their concern when they call us. They're trying to go into issues on their case."

Tricia Bushnell, the MIP's legal director, said that while review of the call data is not yet complete, so far she has been able to locate within the records *The Intercept* provided three calls that were prearranged in the manner the Missouri DOC has said is required.

Still, that may not necessarily reflect the true number of calls within the data that were intended to be privileged — indeed, despite the Missouri DOC's insistence that only prearranged calls would be considered privileged, one Missouri attorney told *The Intercept* that policies governing how attorney-client calls are handled vary from facility to facility within the system, which makes it difficult to determine exactly how many privileged call records are contained within the leaked data.

"Every place is different," Burnette agrees. "Perhaps that's part of the problem, is that there's no standardization." But Burnette says the volume of legal calls included in the hack suggests that the Securus-Missouri DOC call system simply doesn't work — and isn't meeting its duty to protect prisoner rights. "Neither of those organizations are above the law afforded to everyone," he says.

In response to a list of additional questions *The Intercept* emailed to the Missouri DOC, a spokesperson reiterated the agency's initial response — that privileged calls must be prearranged — but added a caveat: "If a requested private call goes past its scheduled time that has been entered into the vendor software, the telephone software system will begin recording the call. At this time, the users will be [given] a notification that the call is being recorded."

* * *

AFTER THE INTERCEPT reported on the Securus hack, the company said there was no evidence that any confidential attorney-client calls were actually recorded. However, the hacker had provided *The Intercept* with several audio files — recordings of actual conversations — that had been downloaded by clicking on the recording URLs within the call records, leading us to draw the logical inference that the other live links were also connected to audio files. Subsequently, Securus appears to have moved the more than 70 million calls in question to a new server, severing further access to the audio files through the links in the data.

Even if an audio file was not available for each of the calls identified by lawyers as confidential, the collection of metadata on those calls is a problem, says the ACLU's Fathi. The database includes names and locations for individual detainees, the date, time, and duration of their calls, as well as the number called and data that appears to indicate how the call was paid for. "You can imagine all kinds of cases where the metadata would itself reveal confidential information," says Fathi.

Burnette agrees that even collecting metadata on attorney-client calls is concerning. "We've talked about this on calls for private citizens — we know what they can glean from metadata," he said. "We know the danger of it — and the value of it. If it wasn't a valuable resource, there wouldn't be Google, right? [With] metadata they know a lot about us."

Take, for example, calls made by detainees to prosecutors — of which we found numerous examples within the data, including calls placed to a U.S. attorney's office in Missouri. "The disclosure that a prisoner called a prosecutor's office could potentially put that prisoner in very great danger," Fathi points out. "If the prisoner were to be, rightly or wrongly, labeled a snitch or informant that could have very serious, and indeed, lethal consequences for the prisoner."

Among prisoners, it is an open secret in Missouri (and, indeed, throughout the criminal justice system) that calls intended to be confidential are monitored and/or recorded by the state. Defense attorney Gipson says that "a lot" of his clients suspect that all of their calls are monitored and/or recorded — despite official assurances to the contrary. "They think that even though it's supposed to be a confidential call, they put [attorney calls] on a line that can be monitored — and then do, I think."

One woman whose husband is housed in a Missouri prison told *The Intercept* that he and his fellow inmates consider it common knowledge that all calls — including privileged communications — are monitored and recorded. According to her husband, she said, at least one fellow inmate related that, while in a court proceeding, prosecutors demonstrated knowledge of information they couldn't possibly have obtained without being privy to communications between the man and his attorney.

This isn't an isolated allegation: In Austin, Texas, a federal lawsuit alleging that privileged calls have been recorded by Securus in the county's jail facilities is currently pending against the company. The lawsuit claims that lawyers there have received copies of their privileged conversations from prosecutors during the evidence discovery process.

The Missouri prisoner's wife also said that it wasn't until December 14, 2015 — more than a month after our initial story was published, but just days after we emailed the DOC a series of questions for this story — that prison officials informed her husband and other inmates of the hack, telling them only that "the system was breached and everyone needed a new PIN" in order to place calls. *The Intercept* obtained a copy of the letter prison officials provided to inmates, which says that the data hacked was "historical call detail records" and did not include any compromising information, such as credit card information or social security numbers. Moreover, the letter reiterated Securus' previous press statements regarding the hack, insisting that there is "no evidence" that attorney-client calls were recorded. "The system has been verified and is working properly," the letter reads.

THE BREACH OF Securus' data in Missouri suggests something larger not only about the mass recording and storage of inmate calls but also about the perils of privatizing core state responsibilities — as is often the case in corrections, where health care, food service, phone service, and even some prison facilities have been privatized. "These are ... services for a population that has very little political power," said Fathi. "So there's not really a lot of care being put into oversight and monitoring and making sure that this service is being provided correctly," he continued. "It continues to be incredible [to me] the sheer scale of what has happened here ... and I think it shows what happens when technological advances and lax oversight come together to produce a bad result of very large proportions."

In fact, the scale of recording and storage of inmate calls by Securus — as well as by its competitors, including industry leader Global Tel*Link — is infinitely larger than represented by the hacked data leaked to *The Intercept.* As of 2012, Securus alone was processing more than 1 million calls per day, from 1,700 facilities serving 850,000 detainees. According to company data provided to *International Business Times*, which ran a friendly profile of Securus CEO Rick Smith last month, the company has now grown to serve more than 1.2 million inmates in 3,450 facilities. The article did not include data on how many calls are currently processed each day, though logic would dictate that the call volume has increased in proportion to the company's expanded reach, from significantly less than 1 million detainees in fewer than 2,000 facilities three years ago to 1.2 million across 3,450 facilities today.

And there is no reason to think that thousands of attorney-client calls, including clearly privileged communications, were improperly recorded only in Missouri and only over a 2 1/2-year period. "Absolutely," says Fathi. "I am 100 percent certain that this is just the tip of the iceberg."

Research: Joshua Thayer

Contact the authors:

Jordan Smith✉jordan.smith@theintercept.com

Micah Lee✉micah.lee@theintercept.com