LISTENING BEYOND THE BARS

New York's Artificial Intelligence Surveillance of Prisoners and their Loved Ones.

ALBERT FOX CAHN, ESQ.

SEPTEMBER 15, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

EXECUTIVE SUMMARY

In 2017, the New York State Department of Correction and Community Supervision (DOCCS) entered into a five-year contract with Securus Technologies, LLC (Securus), a prison technologies firm that delivers pay-per-call telephone services to prisons throughout the United States. The service enables DOCCS to use artificial intelligence (A.I.) to monitor inmates' phone calls. Securus's platform logs and records calls, analyzing conversations with automated voice recognition technology and automated content analysis. This technology purports to identify conversations about illegal activity, but it may simply automate racial profiling and other forms of bias.

Securus Technologies' surveillance products potentially violate inmates' Constitutional rights, and the rights of their friends and family members as well, including minor children. Securus's technology is deeply privacy invasive, but it also is vulnerable to the same sort of A.I. bias that has been documented with facial recognition and other biometric tracking tools.

Key Topics:

- Securus Technologies' voice recognition and identification and monitoring;
- The risk of unauthorized access to the Securus Technologies platform;
- The civil rights impact of Securus Technologies' monitoring; and
- the risk of profiling, bias, and discrimination from Securus Technologies.

In short, the DOCCS's contract with Securus Technologies may subject thousands of New Yorkers to unlawful and discriminatory surveillance, putting them at risk of wrongful arrest.

INTRODUCTION

This white paper summarizes the capabilities of the audio surveillance technology developed by Securus and deployed by DOCCS.

In subsequent sections, we provide an overview of Securus's security protocols and the key concerns associated with the deployment of Securus's surveillance technology in American prisons. These concerns include constitutional issues stemming from the use of computer software in the criminal justice system, and privacy concerns related to insufficient data security protocols.

I. SECURUS TECHNOLOGIES

Securus is a prison technologies firm that provides pay-per-call telephone services for prisons in multiple states across the United States, including Arizona, Florida, Georgia, Texas and Missouri. Securus claims that it provides its services to more than 3,400 public safety, law

enforcement and corrections agencies and over 1.2 million incarcerated individuals across North America.[1] In 2017, Securus entered into a contract with DOCCS to provide an Inmate Telephone System ("ITS") from October 1, 2017 to September 30, 2022, with the option for two one-year renewal periods. Under the terms of the contract, Securus provides DOCCS with an integrated Secure Call Platform ("SCP") through which DOCCS inmates may place outgoing calls. DOCCS officials can access detailed recordings and logs of those calls through the SCP's web-browser-based "facility portal."[2] ITS also provides investigative support for law enforcement, featuring voice recognition and identification capabilities, as well as call monitoring.

a. *Voice recognition and identification*

According to Securus's technical proposal to DOCCS, the SCP can record and monitor inmates' telephone calls using SCP's Investigator Pro ("IPRO") software. Through its voice recognition software, IPRO can identify the name associated with every inmate voice heard during the call, including those of former inmates.[3] IPRO's "searchable voice" feature can then compare dialed parties by voice and identify potential matches across Securus's database. Securus claims IPRO provides "near perfect fidelity," while not substantiating this claim, and has enabled customers to use "information heard through background conversations. "[4]

Because the SCP records all parties to inmate phone calls, it records inmates' friends and family, spiritual advisers, and even minor children. Although IPRO does not identify these innocent bystanders by name, IPRO still samples their voices. Through IPRO's searchable voice feature, investigators can then search for matches to these voice samples across Securus's database, subjecting innocent members of the public to investigation simply for speaking to incarcerated loved ones.[5]

b. *Call monitoring and investigative support*

In addition to identifying parties to a telephone call, Securus also provides live call monitoring and investigative support for law enforcement. The SCP supports real-time, undetectable call monitoring, which Securus manages through its subsidiary, Guarded Exchange. The Guarded Exchange Solution ("GEX") consists of human analysts who can monitor up to seven percent of inmate calls. Securus estimates that this represents a minimum of 1.5 million calls annually and potentially more than ten million calls over the life of Securus's DOCCS contract.[6] In addition to these trained analysts, investigators with security access in the SCP can similarly conduct real-time, undetectable monitoring. They are assisted by the SCP's "covert alert" feature, which alerts an SCP investigator when a flagged inmate places a phone call, and immediately and clandestinely connects the investigator to that call.[7]

[1] SECURUS TECHNOLOGIES, ABOUT US, https://securustech.net/about-us/index.html.
[2] *See* Securus Technical Proposal (January 23, 2017) at 446/771 ("Technical Proposal").
[3] *Id*. at 13/771.
[4] *Id*. at 6/771; 41/771; 55/771.
[5] *Id*. at 13/771.
[6] *Id*. at 13/771; 74-76/771.
[7] *Id*. at 13/771; 74-76/771.

GEX facilitates live analyst and investigative monitoring with an array of real-time investigative technologies including filtering, data mining and behavioral analysis. One example is Securus's THREADS software, which Securus claims can identify trends in inmate calling patterns and then generates targeted investigative leads for law enforcement from these trends that are not subject to external substantiation. These technologies identify "suspicious" key words or phrases, threatening calls and suspected criminal activity. Any "suspicious" calls can then be used to alter Securus's data-mining strategies to meet DOCCS's intelligence-gathering priorities and target specific inmates.[8] Thus, inmates are targeted based on little understood, potentially biased, and even abusive algorithms, generated from nebulous "suspicions." SCP users can also add notes to call logs to establish links between selected inmates and called parties and to identify activities such as gang, drug, victimization, extortion, and other "nefarious activities."[9] Again, Securus's methods for such identification are proprietary and therefore not subject to public scrutiny. Securus calls its THREADS system "[t]he most powerful investigative tool in corrections [and] the easiest to use!"[10]

The SCP provides a limited carve-out for private phone calls, such as those subject to attorney-client privilege, by permitting the designation of certain phone numbers as "private." Private phone numbers are automatically eliminated from all monitoring or recording, and are listed as "private" in call logs.[11] The Technical Proposal is notably silent on the details of how calls are designated as private, who determines such designation, and how Securus is held accountable for following its own protocols. As noted below, Securus has been shown to be recording nominally private calls. The mere knowledge that a privileged call can be recorded is likely to create a chilling effect, deterring inmates from speaking freely with counsel. Further, private calls that are not privileged, such as those with intimate partners, children and clergy are monitored and recorded.

c. *Inconsistent security protocols*

According to Securus's technical proposal to DOCCS, Securus protects telephone call data by constantly monitoring data storage equipment, conducting audits, and maintaining chains of evidence to prevent data tampering.[12] However, Securus designed the ITS to maximize ease of access to recordings and call logs over its obligations to maintain the security of such invasive surveillance technology. Through the facility portal, DOCCS officials can access the SCP remotely on an internet browser with only a username and password and without the need to be on a DOCCS network.[13] SCP users, such as local police departments, can retain recordings indefinitely, keeping recordings on the SCP server for the length of the contract, with the ability to copy recorded conversations onto any external media device connected to the user's personal computer.[14] The ability to access the SCP remotely, combined with the lack of requirements for two factor

[8] *Id*. at 13/771; 74-76/771.
[9] *Id*. at 9/771; 74/771.
[10] SECURUS TECHNOLOGIES, https://securustechnologies.tech/securusthreads.
[11] Technical Proposal at 69/771.
[12] *Id*. at 66/771; 79/771; 107-108/771; 374-377/771; 409-410/771.
[13] *Id*. at 85/771.
[14] *Id*. at 79/771; 81/771.

authentication, leave the SCP and its recordings vulnerable to hackers and other unauthorized users.

II. KEY CONCERNS WITH AUDIO SURVEILLANCE

Key concerns regarding Securus's ITS include (a) personal privacy rights, including those of inmates, former inmates, pretrial detainees, and innocent bystanders, (b) unaccountable software, and (c) flawed data security protections.

a. *Privacy rights*

While prisoners do lose some Fourth Amendment protections and therefore have a lower expectation of privacy than the general public has, they do retain some Fourth Amendment protections.[15] At present, prisoners lack a practical choice as to whether their calls are recorded and whether their voice samples are collected. In most states, the ITS is managed by a single provider that automatically enrolls inmates into the ITS without their knowledge.[16] Securus touts the "[h]igh confidence level in enrollment accuracy" of its "Supervised Enrollment" system, in which "Securus plans, implements, and conducts the entire enrollment with minimal impact on DOCCS, by providing organization and manpower resources to enroll the entire general population."[17] According to Securus's narrative responses to DOCCS's request for proposal, "[s]ince the Securus enrollers validate each inmate via their picture ID and PIN against DOCCS's daily facility roster, there is a confirmed match to all the inmates' enrolled voices. This will give a high level of confidence to DOCCS investigators when performing call-based investigations by inmate voice print and name. Because all inmate enrollment is confirmed and IPRO retains inmates' voice prints after their release, IPRO can later determine and identify an inmate by name, should that inmate become a called party to a current inmate."[18] Anyone wishing to accept telephone calls from incarcerated individuals in New York State correctional facilities is required to have an account with Securus.[19] Alternatively, inmates can be compelled to enroll into ITS against the threat of losing their calling privileges. Even when presented a choice, some inmates consider enrollment "just another thing" they must do in order to call loved ones.[20] This is exacerbated by the notion that prison authorities can decline to post public notices about new surveillance practices, and may fail to inform family members of such changes.[21] Between prisons downplaying the significance of an inmate's choice in this regard, and given the inherently

[15] *See Hudson v. Palmer*, 468 U.S. 517 (1984) (holding that a prisoner has no reasonable expectation of privacy in a prison cell such that he would be entitled to protection under the Fourth Amendment); *see also Samson v. California*, 547 U.S. 943 (2006) (permitting search of a parolee despite lack of suspicion due to the fact that parole is an established variation on imprisonment); *but see Bell v. Wolfish*, 441 U.S. 520, (1979) (requiring that searches of prisoners be reasonable under the circumstances).
[16] *See* George Joseph and Debbie Nathan, *Prisons across the U.S. are quietly building databases of incarcerated people's voice prints*, THE INTERCEPT (Jan. 30, 2019), https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.
[17] Narrative Responses to Requirements (Jan. 23, 2017) 410-411/1014.
[18] *Id.*
[19] DEPARTMENT OF CORRECTIONS AND COMMUNITY SUPERVISION, https://doccs.ny.gov/telephone-calls.
[20] *See* George Joseph and Debbie Nathan, *Prisons across the U.S. are quietly building databases of incarcerated people's voice prints*, THE INTERCEPT (Jan. 30, 2019), https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.
[21] *Id.*

coercive nature of any "choice" a prisoner makes, inmates may not realize the degree of surveillance to which they are "consenting."

The use of such software extends to the collection of voice prints of pretrial detainees who are held while waiting for trial.[22] In other words, Securus monitors the calls of completely innocent people and flags any "suspicious" or "nefarious" conversation for review by investigators. Such conversations could then be leveraged by prosecutors in building their case or negotiating plea bargains. Although pretrial detainees are entitled to the presumption of innocence, recent jurisprudential developments mean that they similarly have "no realistic choice but to divulge information to third parties," in a prejudicial manner.[23] In the recent case of *People v. Diaz*, the use of recordings of pretrial detainees as evidence was ruled admissible so long as the detainee was notified of monitoring.[24] Note that *Diaz* requires notice, not consent. Further, whether charges are eventually dropped or a detainee is found innocent, the voice prints are kept indefinitely.[25] This means that even exonerated inmates will be cycled through a perpetual computer lineup, constantly at risk of false arrest and wrongful conviction if their voice "matches" that of a suspect. Once released, former prisoners must run a bureaucratic gauntlet to expunge their records, first securing a judicial order and then receiving approval from Securus.[26]

Courts disagree whether or not the Fourth Amendment protects biometric information.[27] Further, courts have been slow to respond to the unique privacy harms caused by biometric searches, whether conducted by humans or computers. This judicial failure to respond seems more egregious yet when one examines the impacts of biometric tracking on inmates' friends and families. New York's state privacy protection laws provides a broad carve-out for data collected by the government for law enforcement purposes, and the law does not address government collection of biometric information.[28] While there is a fiction of consent where called parties receive notice that the calls are subject to monitoring and recording,[29] inmates' loved ones often have "no realistic choice but to divulge information."[30] Further, Securus is not divulging the full capabilities of its monitoring when it gives that notice to the innocent called party. Regardless of the legal ambiguity, a system that "criminalize[s] relationships" is intuitively unsettling.[31] An attorney at New York's Legal Aid Society states the problem clearly: "if you have a family member

[22] *See* George Joseph and Debbie Nathan, *Prison tech company is questioned for retaining 'voice prints' of people presumed innocent*, THE APPEAL (Feb. 12, 2019), https://theappeal.org/jails-across-the-u-s-are-extracting-the-voice-prints-of-people-presumed-innocent.
[23] *See* dissenting opinion by Judge Wilson in *People v. Diaz*, 33 N.Y.3d 92, 119 (2019).
[24] *See People v. Diaz*, 33 N.Y.3d 92 (2019).
[25] *See Prison tech company is questioned*, THE APPEAL, https://theappeal.org/jails-across-the-u-s-are-extracting-the-voice-prints-of-people-presumed-innocent.
[26] *Id.*
[27] *See* THE V&E REPORT, *Fingerprints as Testimony: Federal Court Rejects Government Request to Compel Use of Biometrics to Open Digital Devices*, Vinson & Elkins LLP (January 23, 2019), https://www.velaw.com/insights/fingerprints-as-testimony-federal-court-rejects-government-request-to-compel-use-of-biometrics-to-open-digital-devices.
[28] *See* Freedom Of Information Law (FOIL) § 87(2), Personal Privacy Protection Law (PPPL) § 95(5)(a).
[29] *See* Technical Proposal at 134/771.
[30] *See* dissenting opinion by Judge Wilson in *People v. Diaz*, 33 N.Y.3d 92, 119 (2019).
[31] *See Prisons across the U.S. are quietly building databases*, THE INTERCEPT, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.

convicted of a crime, yet you haven't been, why are you now having your information being used for government investigations?"[32]

The severity of these privacy intrusions is illuminated when considering the scale of IPRO's data recording. Securus's database of recorded calls includes millions of recordings that can be stored indefinitely and remain available throughout the life of the contract period.[33] At the end of the contract period, calls must be turned over to a succeeding contractor.[34] These capabilities seem especially problematic when used in conjunction with other police investigative tools. Even though IPRO does not identify the names of called parties whose voice prints are included in the database, it is plausible that police seeking to identify a suspect in a criminal investigation could compare a voice print from Securus's database with a voice captured on a separate wiretap.[35] Thus, it stands to reason that one who accepts a call from an inmate using the Inmate Telephone System risks unwittingly inserting oneself into a police investigation.

Academics have noted that, more than merely "pierc[ing] the veil of anonymity,"[36] the ITS enables the surreptitious capturing of private information. This private information, once captured, potentially can be stored for an indefinite amount of time. Some see a slippery slope between these capturing / storage capabilities and mass surveillance directed toward persons caught up in the criminal justice system and the people they love.

b. *Accuracy and bias*

Others voice concern with what they say is a lack of transparency with respect to how Securus collects and analyzes voice print data. IPRO provides a "voice probability score" that rates the likelihood that an inmate's voice was the voice heard on the targeted call.[37] However, the error rates of IPRO are not publicly known. In the absence of proper oversight, decisions may be made based on faulty voice probability scores. Filtering and data mining techniques tend to struggle with certain accents, dialects, and pitches of voices, exposing minority groups to higher risks of wrongful targeting.[38]

A recent study by researchers at Stanford University found that five automated speech recognition systems, each developed by one of five giant American technology companies, had an

[32] *See* Navanwita Sachdev, *The prison yard becomes a voice recognition playground*, THE SOCIABLE (May 22, 2019), https://sociable.co/technology/prison-yard-becomes-voice-recognition-playground.
[33] *See* Technical Proposal at 78/771; 380/771.
[34] *Id*.
[35] *See Prisons across the U.S. are quietly building databases*, THE INTERCEPT, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.
[36] *See* Oleksandr Pastukhov and Els Kindt, *Voice Recognition: Risks to Our Privacy*, Forbes (Oct. 6, 2019), https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/#71ffa606786d.
[37] *See Prisons across the U.S. are quietly building databases*, THE INTERCEPT, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.
[38] *See* Erin Myers, *The Role of Artificial Intelligence and Machine Learning in Speech Recognition*, Rev (Aug. 25, 2019), https://www.rev.com/blog/artificial-intelligence-machine-learning-speech-recognition; *See also* Rachel England, *Researchers highlight racial bias in speech recognition systems*, ENGADGET (Mar. 24, 2020), https://www.engadget.com/2020-03-24-racial-bias-speech-recognition-siri-alexa-ai.html.

average error rate of 0.35 for Black speakers and 0.19 for White speakers.[39] Despite the flaws inherent to automated speech recognition systems, Securus claims its systems have "higher accuracy," [40] but it has shown publicly no evidence to support that claim.

Low quality recordings of conversations do not allow for "fine-grained distinctions of speech sounds" and generally are not reliable evidence in the context of criminal prosecution.[41] Courts have addressed similar concerns over the accuracy of automated systems. In *State v Loomis*, an algorithmic recidivism risk assessment identified the defendant as a high-risk re-offender, based on aggregate recidivism data of groups of persons "similar" to him.[42] Although the assessment algorithm was a trade secret, the Wisconsin Supreme Court ruled that judicial reliance on the assessment in sentencing did not violate the defendant's right to due process, so long as the assessment came with a written warning and was not the sole basis for the sentencing decision.[43] The court noted, however, that judges likely lack the requisite knowledge to "modulate their consideration of the tool" and may succumb to "cognitive biases supporting data reliance."[44]

In light of IPRO's shortcomings and recent pro-surveillance cases like *People v. Diaz* (recordings of pretrial detainees with notice admissible as evidence), it is not hard to imagine how courts may fail to adequately consider the inherent bias and inaccuracy of the automated systems prosecutors employ.

Some argue that it is only a matter of time before courts must decide whether to allow testimony from systems having artificial intelligence capabilities.[45] The Sixth Amendment's Confrontation Clause guarantees a criminal defendant the right to be confronted with the witnesses against him.[46] This raises the concern of whether, if courts allow artificial intelligence systems to testify in criminal proceedings, can such systems be confronted and cross-examined in a way that is consistent with the Constitution?

c. *Data security protections*

Securus's security protocols have obvious vulnerabilities, despite Securus's claims that its systems provide secure and managed access to call recordings.[47] Significantly, the SCP can be accessed remotely via web browser and from a non-DOCCS network, using just a username and

[39] *See* Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS No. 14, 7684 (2020), *available at* https://www.pnas.org/content/pnas/117/14/7684.full.pdf.
[40] *See* Technical Proposal at 55/71.
[41] *See* Michael Catanzaro et al., *Voice Analysis Should Be Used with Caution in Court*, Scientific American (January 25, 2017), https://www.scientificamerican.com/article/voice-analysis-should-be-used-with-caution-in-court.
[42] See *State v. Loomis*, 2016 WI 68; *See also State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, 130 HARV. L. REV. 1530 (2017), *available at* https://harvardlawreview.org/2017/03/state-v-loomis.
[43] *Id.*
[44] *Id.*
[45] *See e.g.* Katherine B. Forrest, AI AND THE CONFRONTATION CLAUSE, https://www.law.com/newyorklawjournal/2019/05/03/ai-and-the-confrontation-clause/?slreturn=20200719150203.
[46] U.S. CONST. AMEND. XI.
[47] *See* Technical Proposal at 68/771; 70/771; 73/771; 84-89/771; 105-107/771; 369-374/771.

password.[48] Additionally, those with access to SCP may copy recorded conversations to an external media device connected to the user's personal computer,[49] thus increasing the likelihood that sensitive information may be obtained by unintended parties.

In 2015, it was reported that hackers uploaded more than 70 million call records and downloadable recordings of calls obtained from Securus, of which at least 14,000 were "private" calls between inmates and their attorneys.[50] Securus denied the reports and blamed third-party operators over whom it claimed to lack control.[51] In 2016, Securus settled a lawsuit in Texas, where it was alleged that Securus had improperly recorded privileged inmate calls.[52] In 2018, it was reported that hackers uploaded more than 2,800 usernames, email addresses, phone numbers, and scrambled passwords and security questions of Securus users.[53] Further it was noted that in an online user's manual for its products, Securus revealed personally identifiable information of real people.[54] More recently, in 2019 and 2020, Securus settled lawsuits in Kansas and California,[55] again for recording privileged calls, settlements in which it promised to improve on its security protocols and submit biannual compliance reports.

III. CONCLUSION

The audio surveillance of inmates, former inmates, pretrial detainees, and innocent bystanders carried out by DOCCS and Securus raises significant concerns related to potentially unconstitutional invasions of privacy, the trustworthiness and accountability of Securus's computer systems, and data security. Moreover, courts and legislatures have yet to fully appreciate and address these concerns. Until this happens, Securus and the surveillance technologies it employs under the cover of government authority, will continue to operate in legal ambiguity and without adequate oversight and accountability.

---

[48] *Id*. at 446/771.
[49] *Id*. at 81/771.
[50] *See* Jordan Smith and Micah Lee, *Not So Securus, Massive Hack of 70 million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege*, THE INTERCEPT (Nov. 11, 2015), https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients; *See* Jordan smith and Micah Lee, *Not So Securus: Part 2, Lawyers Speak Out About Massive Hack of Prisoners' Phone Records*, THE INTERCEPT (Feb. 12, 2016), https://theintercept.com/2016/02/12/not-so-securus-lawyers-speak-out-about-massive-hack-of-prisoners-phone-records.
[51] *See* Technical Proposal at 465-466/771.
[52] *See* Jordan Smith, *Securus settles lawsuit alleging improper recording of privileged calls*, THE INTERCEPT (Mar. 16, 2016), https://theintercept.com/2016/03/16/securus-settles-lawsuit-alleging-improper-recording-of-privileged-inmate-calls.
[53] *See* Joseph Cox, *Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US*, VICE, (May 16, 2018), https://www.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked.
[54] *Id*.
[55] *See* Dan Margolies, *Leavenworth Inmates Reach $1.45 Million Settlement Over Taped Attorney-Client Phone Calls*, High Plains Public Radio (Aug. 26, 2019), https://www.hppr.org/post/leavenworth-inmates-reach-145-million-settlement-over-taped-attorney-client-phone-calls; Brigette Honaker, *Securus Prison Call Recording Class Action Settlement Gets Ok*, TOP CLASS ACTIONS (Jun. 22, 2020), https://topclassactions.com/lawsuit-settlements/lawsuit-news/jail-prison/securus-prison-call-recording-class-action-settlement-gets-ok; *See* Maeve Allsup, *Inmates, Attorneys Settle California Prison Call Recording Suit*, BLOOMBERG LAW (Jun. 17, 2020), https://news.bloomberglaw.com/us-law-week/inmates-attorneys-settle-california-prison-call-recording-suit.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT