

Exhibit 22

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF BRONX

Matter of Marcus Reid, Eric Leon, Tyrell Scott, Lillian
Nelson, and Samiyah Defreitas,

On behalf of themselves and all others similarly situated,
Petitioners,

For a judgment under Article 78 of the Civil Practice
Law and Rules

--against--

NEW YORK CITY DEPARTMENT OF
CORRECTION,

Respondent.

**AFFIRMATION BY
ATTORNEY ELIZABETH
DANIEL VASQUEZ IN
SUPPORT OF VERIFIED
ARTICLE 78 PETITION**

I, Elizabeth Daniel Vasquez, an attorney admitted to practice law before the courts of the State of New York, and not a party to the above-certified cause of action, affirm pursuant to CPLR § 2106 and under penalties of perjury as follows:

1. I am the Director of the Science and Surveillance Project at Brooklyn Defender Services (“BDS”). I am a member in good standing of the bar of the State of New York.

2. BDS is a full-service public defender 501(c)(3) organization that provides multi-disciplinary and client-centered criminal defense, family defense, immigration, and civil legal services, along with social work and advocacy support. BDS represents low-income people in nearly 22,000 criminal, family, civil, and immigration proceedings each year. BDS represents hundreds of people detained or incarcerated in New York City’s jails at any time.

3. As the Director of BDS’s Science and Surveillance Project, I lead the office’s litigation and advocacy work surrounding issues of data, science, and technology, providing direct case consultation, training, and client representation.

4. BDS’s Science and Surveillance Project began in 2020. Since that time, my team has been investigating the New York City Department of Correction’s (“DOC”) use of

surveillance tools on New Yorkers, DOC's relationship with Securus Technologies, Inc. ("Securus"), and Securus' products and technical capabilities.

5. This declaration is based on publicly available materials, documents received in response to numerous Freedom of Information Law requests, as well as my personal knowledge, gathered through my own experiences, supervision of staff in BDS's Criminal Defense Practice and Science and Surveillance Project, and coordination with the other leaders of BDS's practice areas. I also regularly consult and coordinate with practitioners at defender organizations in New York City, New York State, and across the country.

A. The Evolution of Phone Service in Jails and Prisons

6. The installation of commercial payphones in United States jails and prisons began in earnest in the mid-1970s.¹ Nationwide, officials rolled out phone programs guided by research that showed community contact for incarcerated people reduced recidivism.²

7. As with most telecommunications services in the United States, AT&T monopolized the market for jail and prison payphones until its break-up in 1984. The break-up of AT&T's Bell system opened the space to new competitors, and dramatically shifted the focus of what had been a purely payphone and operator-assisted collect calling market.³

8. Because the government entities that run carceral facilities have "uniquely effective monopoly sourcing power," companies in this specialized communications market—increasingly, dedicated start-ups and retooled equipment companies—began "exchanging

¹ See Steven J. Jackson, *Ex-Communication: Competition and Collusion in the U.S. Prison Telephone Industry*, 22:4 *Critical Studies in Media Communication* 263, 267 (Oct. 2005).

² See, e.g., Don Adams and Joel Fischer, *The effects of prison residents' community contacts on recidivism rates*, 22 *Corrective & Social Psychiatry & Journal of Behavior Technology, Methods & Therapy*, 4, 21-27 (1976).

³ Jackson, *supra* n.1, at 268.

exclusive service rights for large commissions paid back into state funds.”⁴

9. Large commissions, fees, and captive market forces served to artificially inflate calling prices for those incarcerated and their families and loved ones. The price of phone calls from jails and prisons peaked in the 1990s and began to face organizing pressure from community groups in the early 2000s.⁵

10. At the same time that resistance to rising costs began coalescing, a new form of market investment—private equity—began to dominate American business. Private equity relied on burdening a company with debt and expanding the company through a strategy of aggressive buyouts of ancillary businesses.⁶ Private equity investment tended to favor businesses that featured technology products and innovation and looked for markets that were resistant to recession; these criteria made the carceral communication industry particularly attractive.

11. Securus was born out of the merger of two smaller corrections telecom corporations in 2004, orchestrated by the private equity firm H.I.G. Capital.⁷

12. Soon, two of the companies funded by private equity firms—GlobalTelLink (“GTL”) and Securus—held more than three quarters of the carceral communications market.⁸ They combined progressively higher fees with a data-driven business model.

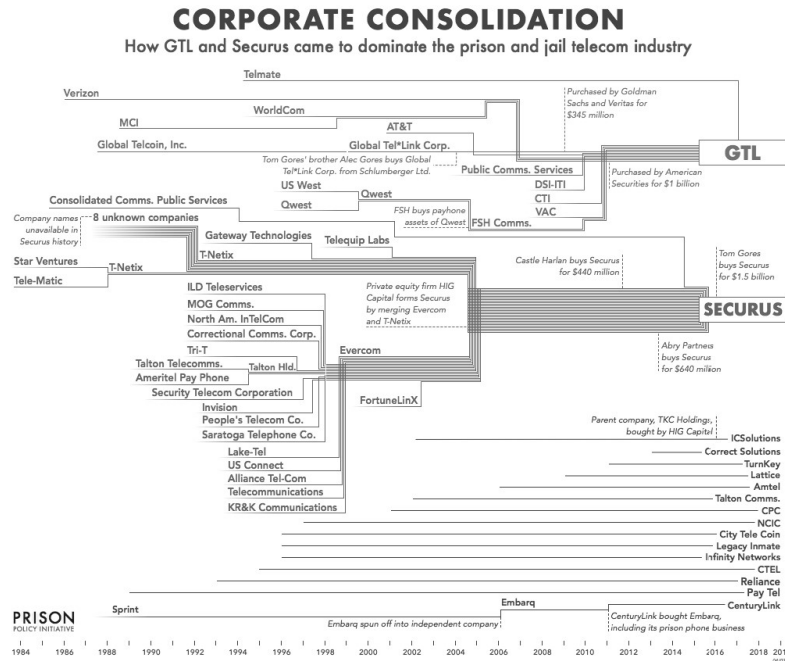
⁴ *Id.* at 268-69.

⁵ *Id.* at 273-77.

⁶ Sandeep Singh Dhaliwal, *Investing in Abolition*, 112 GEO. L.J. 1, 9-14 (2023).

⁷ Business Wire, *HIG Capital Completes Sale of Securus Technologies*, Nov. 10, 2011, <https://www.businesswire.com/news/home/20111110005790/en/H.I.G.-Capital-Completes-Sale-of-Securus-Technologies>.

⁸ See Kalena Thomhave, *Prison Advocates Declare Win as Proposed Prison Phone Industry Merger Dies*, April 4, 2019, <https://prospect.org/justice/prison-advocates-declare-win-proposed-prison-phone-industry-merger-dies/>; Prison Policy Initiative, *Corporate Consolidation: How GTL and Securus came to dominate the prison and jail telecom industry* graphic (updated April 3, 2019).



B. New York City Jails' Phone Service Programs

13. Meanwhile, in New York City, phone service for use by incarcerated people was installed in Rikers Island between 1970 and 1980.⁹ Phone service was originally provided by the local New York Telephone Company.¹⁰

14. Encouraged by the Board of Correction (“BOC”), DOC originally provided local phone calls free of charge and did not monitor or record phone calls without a warrant.¹¹ Instead, BOC and DOC emphasized the importance of community communication for those detained.¹²

⁹ BOC, *Meeting Minutes* (Oct. 30, 1970) (“Among the principal changes being worked on is phones so inmates can make unmonitored outside calls.”); BOC, *Minimum Standards* (1978) (“11. Telephone calls. Prisoners are entitled to make periodic telephone calls.”).

¹⁰ See, e.g., BOC, *Meeting Minutes* (Jan. 8, 1973) (referencing DOC pursuing phone installation throughout its various facilities with the New York Telephone Company).

¹¹ BOC, *Minimum Standards*, § 11.8, (1978) (“*Supervision of telephone calls*. Prisoner telephone calls shall not be listened to or monitored except as to time and cost, unless a lawful warrant is obtained.”).

¹² See, e.g., BOC, *Meeting Minutes* (June 10, 1974) (“It was noted in general how difficult it was for visitors to get to Rikers Island and, once there, to be cleared to go to the institutions. Also noted generally was the lack of inmates’ access to telephones. Mr. Brickman urged that the Board’s report should be strong in calling for the installation of telephones on Rikers Island as quickly as possible.”); BOC, *Meeting Minutes* (Feb. 11, 1971) (“The Chairman then informed the Board that he would like its approval to announce publicly . . . an ‘Agenda for Action,’ . . . [that]

15. By 1978, BOC issued its first set of Minimum Standards governing DOC facilities, which included a right of access to periodic telephone calls.¹³

16. By 1999, DOC was generating a reported \$2.4 million in revenue from a surcharge applied to calls after the first call was made and paid by those incarcerated or detained and their families.¹⁴

17. Almost a quarter century after phone calls came to New York City jails, DOC began campaigning for permission to circumvent eavesdropping laws and universally record all phone calls in its facilities. More specifically, in 2003, DOC requested that the BOC lift the warrant requirement for listening in on phone calls to allow them to record and monitor calls in DOC facilities. BOC expressed skepticism, pointing specifically to both privacy concerns and the issue of attorney-client privilege. BOC rejected DOC's request, requiring detailed answers to its questions around these issues before it would consider the proposal.¹⁵

18. Three years later, DOC again asked BOC to allow the recording and monitoring of phone calls from the jails, which was strongly supported by several New York District Attorneys.¹⁶

19. After much discussion and a particular emphasis on protecting the confidentiality

would call on the community to show its good faith in helping to improve the conditions in the prisons. For example, the Telephone Company would be urged to expedite phone installations in the prisons.”); BOC, *Meeting Minutes* (Oct. 30, 1970) (“Among the principal changes being worked on is phones so inmates can make unmonitored outside calls.”).

¹³ BOC, *Minimum Standards*, § 11.1 (1978) (“Prisoners are entitled to make periodic telephone calls.”).

¹⁴ BOC, *Meeting Minutes* (Dec. 8, 1999) (“[Assistant Chief Psomas] said that DOC generated \$2.4 million in revenue from a 25-cent surcharge on telephone calls. Mr. Schulte asked why the surcharge was imposed. Assistant Chief Psomas said it was to pay for the system. Deputy Commissioner Thomas Antenen added that the surcharge only applied to calls made after an inmate first received a free telephone call.”).

¹⁵ See BOC, *Meeting Minutes* (Oct. 9, 2003).

¹⁶ See BOC, *Public Hearing on Proposed Amendments to Minimum Standards for New York City Correctional Facilities* (April 17, 2007) (including request from then-DOC Commissioner Martin F. Horn for permission to record jail phone calls).

of attorney-client phone calls, the Board amended the Minimum Standards: “The Board voted to amend subdivision (h), authorizing the Department, upon implementation of appropriate procedures and legally sufficient notice to prisoners, to listen to and monitor prisoner telephone calls, except for telephone calls to the Board of Correction, Inspector General, other monitoring and investigative bodies, treating physicians and clinicians, attorneys and clergy.”¹⁷

20. The new minimum standards permitted DOC to set up a technical system for conducting listening and monitoring of telephone calls made by incarcerated people. At that time, in 2007, correctional facilities still predominantly relied on analog recording methods to monitor calls, such as tape recorders and physical wiretaps. But digital methods were on the very near horizon, and the landscape for call monitoring was changing. BOC’s debate surrounding the rule change reflected this, as BOC repeatedly indicated that the technical details of implementation remained to be resolved.¹⁸

21. At the same time, BOC made clear that attorney-client calls were to be sacrosanct: neither listened to (physically or digitally) or monitored in any way.¹⁹ DOC was tasked with implementing the protection for the monitoring of privileged calls in its operating orders, which would then be reviewed by BOC for compliance with the minimum standards.

22. BOC’s new standards became operative on June 16, 2008.

23. Since the beginning of DOC’s surveillance system, information from recorded phone calls was used almost exclusively by prosecutors to prosecute existing criminal cases,

¹⁷ BOC, *Minimum Standards*, § 1-10 (2007).

¹⁸ See, e.g., BOC, *Meeting Minutes* (May 10, 2007) (extending the deliberative process for the minimum standard amendments and noting that “[t]he Board has not researched new technologies that are available to address issues that are before the Board for consideration. What are the technologies available to monitor inmate telephone conversations?”); BOC, *Meeting Minutes* (July 10, 2008).

¹⁹ See, e.g., BOC, *Meeting Minutes* (Nov. 8, 2007) (discussing “how . . . privileged phone calls [are] going to be kept sacrosanct” and complaining that this point has not been technically resolved or explained by BOC or DOC).

rather than by DOC to promote safety in the jails. In March 2009, then-DOC Commissioner Martin F. Horn reported to the BOC on the new universal call recording program:

He said 100,000 phone numbers are registered as confidential, primarily attorney numbers. He reported that 2 million phone calls have been recorded, with copies of recordings requested as follows: 1900 subpoenas filed by assistant district attorneys, five requests from the New York Police Department, two requests from the United States District Court in New Jersey, and one request from U.S. Attorney's Office Southern District. He said that only 114 requests were made by DOC staff despite his pressing staff to make more use of taped information . . . He reminded the Board that it was the District Attorney's Offices that most strongly supported the amendment to permit taping phone calls and that the DAs say the tapes promote public safety.²⁰

24. Between 2008 and 2014, DOC administered its internal phone system by contracting with Verizon.²¹

25. To add surveillance and billing-management capabilities on top of its regular phone system, DOC built two custom software applications: (1) a program that managed verification of caller identity, accounting of funds to pay for the call, and rules for individual calls (e.g., imposing time and called party limitations) while also handling the tracking of recordings; and (2) a program that managed the provision of voice announcements, like the warning that calls may be recorded.²²

26. Responding to the BOC's clear concerns around privileged calls and protecting civil liberties, from 2008 through 2016, DOC's Operations Orders on phone recording emphasized stringent protocols to establish a list of numbers associated with privileged communications that the Department termed the "Do Not Record List" and to regulate accessing

²⁰ BOC, *Meeting Minutes* (May 14, 2009).

²¹ DOC, *Request for Proposal ("RFP") for the Inmate Phone System*, PIN: 072201315MIS, at 5 (May 13, 2013).

²² *Id.* at 4.

or listening to call recordings more broadly.²³

27. For example, the Inmate Telephone Recording & Monitoring Operations Orders began with the “Policy” that “The Department shall record all inmate telephone calls and retain those recordings, except for those telephone numbers of persons or agencies that appear on the ‘Do Not Record List’”²⁴ The Policy section continued with specific rules for generating, managing, and enforcing the Do Not Record List.

28. While DOC’s policy was to record all nonprivileged calls, initially a higher level of scrutiny was required before any call recording could be accessed or listened to. The 2008 and 2009 versions of the Order laid out “Procedures” for the recording and monitoring program that delineated, among other things, “Authorization to Record and Monitor Inmate Telephone Calls,” which required executive level approval from one of six high level staff to access or listen to a call recording.²⁵

29. Less than ten years after BOC did away with the warrant requirement for recording and monitoring phone calls made by people in DOC custody, DOC fundamentally changed the call recording program again. This time, DOC used the narrow permission it had received to listen to phone calls to transform an internal security program into a broad intelligence-gathering surveillance regime that targets communities far outside the walls of its jails.

C. To Achieve a Surveillance Regime, DOC Contracts with Securus Technologies

30. In the spring of 2013, DOC issued a Notice of Solicitation Request for Proposal (“RFP”) “seeking a qualified vendor to establish a contract for furnishing, installation, operation,

²³ See DOC Operations Order: *Inmate Telephone Recording & Monitoring*, effective June 26, 2008; DOC Operations Order: *Inmate Telephone Recording & Monitoring*, effective March 9, 2009.

²⁴ *Id.*

²⁵ *Id.*

and maintenance of a new Inmate Phone System (IPS) together with associated phones and cabling, and to replace the existing system in the Agency's facilities." DOC claimed that a new system would "result in significant benefits to the Department, including reduced or no cost of ownership . . . [and] use of latest technologies providing more comprehensive features" ²⁶

31. Among the key requirements outlined in the RFP was that the new system "[a]uthenticate inmates in a reliable manner by using advanced biometric[s]," such as voiceprint, fingerprint, iris scan, or RFID wristband. ²⁷ DOC also outlined several minimum requirements, including that the system "should, by default, record all telephone calls." ²⁸

32. While emphasizing its desire for advanced biometrics, the latest technologies, and enhanced investigative functions, the RFP did not include among its requirements protections for confidential communications or guaranteed access to legally privileged calls. The RFP only mentioned a "Do Not Record" List five times in its more than 200 pages. Despite the BOC's emphasis on the need for unrecorded telephone access to lawyers, medical professionals, clergy, and the BOC itself, the RFP did not mention protections of these phone calls at all.

33. Bids on the RFP were due by June 18, 2013, and DOC received bids from several companies.

34. In the fall of 2013, after a preliminary vetting process, DOC invited three finalists—GTL, Securus, and Telmate—to present their Best and Final Offer ("BAFO"), and asked that each BAFO include the following information: (1) All features and services included in the base price / revenue structure; (2) Exclusion of any "non-commissionable" components;

²⁶ DOC, *Request for Proposal (RFP) for the Inmate Phone System*, PIN: 072201315MIS, Notice of Solicitation (May 13, 2013).

²⁷ *Id.* at 6.

²⁸ *Id.* at 9.

(3) Inclusion of Transcription Services for a minimum of 10% of all calls.²⁹

35. DOC's BAFO request also explicitly highlighted DOC's perception that the agency existed within a unique oversight environment and expressed reservations about responding to public criticism of the commission rate it would receive. The tone and tenor of DOC's BAFO request provided hints that it would seek political protection from its contractor's public relations apparatus and political cover for its questionable new foray into the broader correctional surveillance market.³⁰

36. All three companies responded. In its BAFO, Securus emphasized the intelligence options it was providing to DOC, including "voice biometric identification," "2 full time site administrators/technicians," "1 full time investigative specialist for staff support, analysis and data integration . . .," and the "Threads Data Analytics Program currently used by [the NYPD] including integration capabilities with Palantir."³¹ As discussed in more detail below, THREADS is Securus's flagship analytic surveillance tool used by law enforcement for finding and sharing relationships and patterns among large amounts of biometric and other personal data.

37. In 2014, DOC selected Securus as its vendor. From the beginning, the relationship between DOC and Securus centered on Securus's ongoing offers to provide the latest advanced data collection technologies to DOC free of charge.³²

²⁹ GTL, *Best and Final Offer*; Securus, *Best and Final Offer ("BAFO")*; Telmate, *Best and Final Offer*, Sept. 27, 2013.

³⁰ *Id.*, Question 1 ("NYC DOC is unlike any other correctional jurisdiction, with multiple oversight agencies including the New York State Commission of Correction at the State level and the NYC Board of Correction at the City level. Additional influential stakeholders may also include the NYC Mayor's office and various inmate advocacy groups. Your cost proposal may...effectively increase the costs to NYC DOC inmates and may prompt concerns from these groups. Please include in your Best and Final Offer ("BAFO") a statement as to how you would respond to oversight agency requests for a reduction or cap of costs to inmates, as well as current and potential future FCC rulings, without impacting the Commission Rates offered to NYC DOC").

³¹ Securus, *BAFO*, at 2-3.

³² *See, e.g., id.* at 4 ("Securus will also provide the City of New York with: JLG Continuous Voice Verification and

38. After hiring Securus and despite the many red flags about Securus's ability to honor basic legal and constitutional requirements, in 2016, DOC again edited its Operations Order covering call recording and monitoring to prioritize intelligence gathering to benefit external law enforcement agencies over respecting confidential communications.³³

39. The contract was for a five-year term, with five subsequent one-year renewal options.³⁴

40. The initial contract listed a set of products Securus intended to provide DOC. Even in 2014, these specifically included (1) the Secure Call Platform with quarterly upgrades, (2) Voice Biometric Identification of Every Inmate *and* Continuous Voice Verification and Identification with Investigator Pro," and (3) "Reverse Look Up with mapping."³⁵ Later amendments to the contract and upgrades included new products, like THREADS.³⁶

41. The following sections of this affidavit will explain what each of these product offerings is and explore how they individually and collectively impact New Yorkers. These products enable a far-reaching surveillance system that sweeps up the personal data not only of people in DOC custody, but also of their loved ones in the community and enables the sharing of that data with law enforcement.

Identification with Investigator Pro – Our partner solution will provide the identification of multiple inmates on a single call without pausing the call for re authentication... Video Capture Capabilities as deployed at the Connecticut Department of Correction to permit the association of a video and photo capture with each inmate during the booking process in addition to our voice verification biometric capabilities").

³³ DOC, Operations Order: *Inmate Telephone Recording & Monitoring*, effective June 10, 2016.

³⁴ City of New York, Dep't of Correction, Agreement for the Installation, Configuration and Maintenance of an Inmate Telephone System, with contractor Securus Technologies, Inc. (hereinafter, "DOC-Securus Contract"), § 2.1 (July 2014).

³⁵ *Id.*, Appendix B, at 1-2.

³⁶ *See, e.g.*, Amendment No. 5 to the Agreement Between DOC and Securus, signed Jan. 17, 2023, Exhibit 1.

D. Securus's Jail Surveillance Products Target Communities

1. The Secure Call Platform

42. In 2007, when Securus was relatively new, it introduced what would become the backbone of its product offerings: the Secure Call Platform (“SCP”).³⁷

43. The Secure Call Platform handled Securus’s mundane, bread-and-butter business: the provision, management, and billing of phone calls.

44. Securus’s innovation came when it transitioned the Secure Call Platform from analog phone service to digital transmission, paving the way for a new model of surveillance.

45. The digital SCP brought two big changes. First, Securus could remotely store and access data from every jurisdiction it serviced, as well as remotely push updates to its Secure Call Platform. Second, by digitally collecting all available data in one computerized platform, big data analysis became possible for Securus and its corrections industry customers.

46. Since 2014, DOC has used the Secure Call Platform to digitally transmit, manage, and store all calls people in custody place to the community.³⁸

47. Between 2012 and 2015, Securus went on a “relentless debt-fueled buying spree, grabbing hold of numerous ‘complementary’ companies.”³⁹ During this period, Securus added companies that provided video visitation, payment processing services, GPS monitoring, data analytics and investigative tools, and continuous voice biometric analysis.⁴⁰ These buyouts quickly paved the way for new product offerings. Securus issued press releases throughout the

³⁷ Securus, *History*, <https://securustechnologies.tech/about/history/>.

³⁸ See DOC-Securus Contract, *supra*, n.35. While the storage of calls *should* exclude privileged communications under the BOC minimum standards and the law, DOC and Securus have failed to comply with this legal mandate; thus, we have chosen “all calls” in this sentence intentionally.

³⁹ Dhaliwal, *Investing in Abolition*, *supra* n.6, at 23-24.

⁴⁰ *Id.*; Securus Technologies, *History*, <https://securustechnologies.tech/about/history/>.

2010s, lauding, for example, its “diversified, government services, high-tech, high software content business” model and its “expansion into [multiple new] vertical markets.”⁴¹

48. Because DOC’s contract term included free quarterly updates of the Secure Call Platform, DOC received each product enhancement and upgrade to the SCP that Securus rolled out.⁴²

49. By 2018, Securus had expanded the purpose and function of its Secure Call Platform—renamed the NextGen SCP—from a computer-mediated phone system into a tool to collect, store, and mine data. NextGen SCP is a cloud-based database that houses multiple streams of Securus-collected data, including (a) call recordings, (b) machine transcriptions of the call recordings, (c) extensive data provided by the carceral facilities about the incarcerated people placing the calls, and (d) billing name and address records for recipients’ landlines. Thus, DOC’s NextGen SCP contains all of this data for each call made by a person in custody to their family, friends, and community.

50. The original Secure Call Platform was indexed by multiple fields but was largely structured around a unique Personal Identification Number (PIN) that was assigned to each person in custody and had to be entered before placing any call. The NextGen SCP has incorporated continuous voice verification, increasing the data mining potential of recorded phone calls. In launching the NextGen SCP, Securus boasted: “This is not just a new calling platform, it’s a single interface that allows you to manage every inmate interaction and gain more intelligence

⁴¹ See, e.g., Securus Technologies, *Securus Transforms Business from Incarcerated Individual Telecom Only to Diversified, Government Services, High-Tech, High Software Content Business* (Oct. 12, 2016), <https://securustechnologies.tech/securus-transforms-business-from-inmate-telecom-only-to-diversified-government-services-high-tech-high-software-content-business/>.

⁴² See DOC-Securus Contract, *supra*, n.35.

than ever before.”⁴³

2. Continuous Voice Verification and Voiceprints

51. Securus conceived continuous voice verification in response to the advent of cell phones and in an effort to gather information on community members who are contacted by people in custody. When landlines were in primary use, the identity and physical location of a called party was easy to obtain and relatively reliable through industry-standard billing name and address (“BNA”) records. Cell phones changed this situation, as they did not have an industry agreed upon standard BNA record.⁴⁴ No longer could Securus (or any other entity) quickly identify the person being called or their location by merely pulling the record associated with that phone number.

52. To fix one aspect of this data gap, Securus introduced continuous voice verification. The tool relies on a form of biometric identification: the digital capture and mapping of unique patterns in voice and speech, which can be used to generate “voiceprints.” Those voiceprints can then be applied to a call recording to identify people who are speaking.

53. Securus marketed continuous voice verification as a “security” product to verify that a person in custody was using the PIN assigned to them. However, Securus does not merely deploy continuous voice verification to confirm that a detained caller’s voice matches the PIN number entered at the start of a call; rather, the capture of voiceprints adds an additional unique identifier to Securus’ call record database. Unlike the PIN, which only allows for calls to be indexed in the database by the associated *detained* caller, capturing voiceprints from the call

⁴³ Securus, NextGen SCP, Promotional Video, <https://vimeo.com/292980872> (uploaded Oct. 2, 2018).

⁴⁴ *See, e.g.*, Securus Technologies, Location Based Services (LBS) Securus White Paper, at 1 (Feb. 21, 2018), https://www.eff.org/files/2018/05/03/securus_white_paper_location_based_services_lbs_copy.pdf (“Currently over 80% of United States citizens are using their cellular phone as their primary form of communication. Therefore, the relevance of traditional billing name and address (BNA) collected through registered land line phone numbers no longer applies.”).

recording allows for biometric data to be collected and indexed from the *recipient* of carceral calls, as well.

54. Continuous voice verification, therefore, is a tool to identify and monitor not merely activity *inside* of detention facilities, but more specifically thoughts, communication, and relationships *outside* of those facilities within the broader community.

55. As Securus explained, it “purchased JLG Technologies in June of 2014 and . . . fully integrated their technology into [their] SCP inmate calling platform because [they] . . . recognized that voice biometric technology had evolved beyond just periodic re-verification of an inmate’s voice to a more advanced continuous **voice identification** of all callers participating in the call.”⁴⁵

56. In 2016, Securus issued a press release explaining the importance of voice biometric technology: “[T]he new software gives investigators the ability to select a voice sample from either the Incarcerated Individual or called party side of an Incarcerated Individual’s telephone call and then use that sample to search for all other calls where that voice occurs. . . . The searchable voice feature makes it possible to follow the individual voice, not just the PIN/ID or telephone numbers. An investigator can now answer questions like these: What other Incarcerated Individuals are talking to this particular called party? Was this called party ever an . . . Incarcerated Individual?”⁴⁶

57. As a component of Securus’s NextGen SCP, continuous voice verification is deployed by every carceral facility that contracts with Securus for phone services. Ultimately,

⁴⁵ FCC Ex Parte Submission, WC Docket No. 17-126, ITC-T/C-20170511-00094, ITC-T/C-20170511-00095, at 42 (Aug. 2, 2017).

⁴⁶ Securus, *Securus’ JLG Technologies Releases Investigator Pro 4.0* (Sept. 7, 2016), <https://securustechnologies.tech/securus-jlg-technologies-releases-investigator-pro-4-0/>.

without notice or warning, Securus is using its call platform to amass a vast biometric database populated by voiceprints unknowingly collected from members of the community whose only connection to the criminal legal system is their association (familial, personal, or otherwise) with someone who is incarcerated or detained.⁴⁷

58. As shown in the RFP, Securus' BAFO, and the 2014 DOC-Securus contract, DOC specifically contracted with Securus to receive continuous voice verification services. Since 2014, voiceprints have been collected from countless New Yorkers including both those detained within DOC's facilities and those communicating with them from the community at large.

3. Location Based Services

59. As Securus laid out in a 2018 white paper, the rise of cell phones not only impacted how to identify a called party, but also how to identify their location: "Due to the shift to cellular phone communication, the ability to understand a called parties' location has become increasingly unclear."⁴⁸

60. To answer this shift, Securus introduced Location Based Services (LBS) into its NextGen SCP. LBS provided another data stream pulled from recorded calls that could be collected, analyzed, and mined to broaden the web of community surveillance.

61. When the called party was using a cell phone, Location Based Services "replaced" "[t]he legacy billing name and address data that was once applicable" "with the delivery of

⁴⁷ Securus has explained that continuous voice verification of *called* parties leverages the entirety of Securus' collected data, not merely the data available in the individually monitored call; notwithstanding later attempts to clean up this admission in the press. Securus's patent application describing an invention that would detect unauthorized three-way calling, for example, noted that it worked by "listen[ing] to all of the voices engaged in the call," "[u]sing information gathered from the voices," and applying "certain voice characteristics data for the resident and voice characteristics data for the outside called party [which] might have been previously gathered during earlier calls or at the beginning of the current call." Robert L. Rae, Michelle L. Polozola, and John S. Hogg, Jr., *Unauthorized call activity detection and prevention systems and methods for a voice over internet protocol environment*, United States Patent Application Publication No. US 2011/0110367, 0045 (May 12, 2011).

⁴⁸ Securus, Location Based Services (LBS) White Paper, at 2 (Feb. 21, 2018).

latitude and longitude of cellular devices.”⁴⁹

62. While Securus marketed Location Based Services as specific to facility calls—allowing investigators to identify the location of parties called by those within the facility—and thus allegedly targeted to enhance security, the “On Demand Search” feature permitted an investigator logged into NextGen SCP to identify the location of any cell phone in use in the United States.

63. DOC specifically contracted with Securus to receive this service under the product “Reverse Look Up with Mapping.”⁵⁰

64. Even in 2014, when DOC first contracted with Securus and four years before the United States Supreme Court concluded in *Carpenter v. United States* that this kind of warrantless location surveillance is illegal,⁵¹ DOC’s participation in this surveillance program was already clearly illegal under New York law. The New York Court of Appeals recognized, as early as 2009, that the New York State Constitution prohibited long-term, technologically mediated, warrantless location tracking by the State.⁵² DOC contracted for this surveillance service despite its illegality.

65. It was only in 2018, when Securus stopped offering Location Based Services following *Carpenter* and adverse political pressure and press attention,⁵³ that DOC lost access to the product.

⁴⁹ *Id.*

⁵⁰ DOC-Securus Contract, *Appendix B*, at 2.

⁵¹ 585 U.S. 296, 320 (2018).

⁵² *See People v. Weaver*, 12 N.Y. 3d 433, 447 (2009).

⁵³ *See, e.g.,* Stephanie Lacambra and Jennifer Lynch, *Senator Wyden Demands Answers from Prison Phone Service Caught Sharing Cellphone Location Data*, Deeplinks Blog (May 11, 2018), <https://www.eff.org/deeplinks/2018/05/senator-wyden-calls-fcc-investigate-real-time-location-data-sharing-all-cellphone>.

66. Thus, for at least four years, DOC's surveillance system included extensive location data for cellphones throughout New York and the country.

67. Securus's incorporation of both continuous voice verification and location-based services in its NextGen SCP were specifically aimed at collecting, storing, and mining data about the recipients of carceral communications, creating a broad community-targeted surveillance system. By contracting with Securus for these products and utilizing these services, DOC constructed and obtained access to a broad community-targeted surveillance system. The extensive voiceprint database houses and analyzes biometric data from countless New Yorkers and, at one time, incorporated exhaustive location-based records from New Yorkers' cellphones. However, neither Securus nor DOC stopped with biometric or location-based surveillance.

4. National Dataset Aggregation through THREADS

68. After Securus acquired DirectHit Systems in 2012, it explained that its acquisition of "a provider of sophisticated investigative, data analysis tools for law enforcement and corrections" meant that Securus could "expand [its] security features/products." Specifically, Securus aimed to acquire DirectHit's featured product, THREADS.⁵⁴

69. At the time of acquisition, THREADS was a patented cell phone analysis tool. Securus's interest in THREADS stemmed from the system's algorithmic solution for finding relationships and patterns among large amounts of call-related data. THREADS patented analytics were specifically tuned to culling call-related data for insights about call participants' social networks, call patterns, and communication substance.⁵⁵ Securus's innovation lay in

⁵⁴ Securus, *Securus Technologies, Inc. Announces Acquisition of DirectHit Systems, Inc. (THREADS™ Product)* (July 3, 2012), <https://www.prnewswire.com/news-releases/securus-technologies-inc-announces-acquisition-of-directhit-systems-inc-threads-product-161229665.html>.

⁵⁵ Securus, *Securus THREADS*, <https://securustechnologies.tech/securusthreads/> ("Using THREADS inner circle reporting option, investigators can see a web of individuals that inmates are contacting in a pattern, and display the

applying THREADS not merely to siloed, individual cell phone data, but instead to its vast data repository of call detail records, call recordings, and other data streams.

70. Following its addition of THREADS to its suite of products, Securus focused its marketing on the claim that its “Securus Call Platform (SCP), combined with THREADS, is unequivocally the largest centralized data repository and most powerful analysis software on the market for both corrections and law enforcement.”⁵⁶

71. For Securus, THREADS represented an opportunity to expand its customer base beyond corrections agencies, allowing Securus to sell subscription-based access to both its data analytics tool and its broad data repositories directly to city, county, state, and national law enforcement and intelligence agencies.

72. THREADS targets those who are not detained, incarcerated, charged with any crime, or even being investigated. The data collected within that system—once nationally aggregated—expands the system’s focus from a purely internal field of view to a broader community cataloguing tool.

73. In 2017, Securus publicly reported that its THREADS database included data from more than 1.55 million incarcerated and non-incarcerated people. Securus bragged that it “has the most widely used platform in the industry, with approximately 2,200 facilities installed, over 1 million inmates served, literally petabytes of intelligence data, and over 1 million calls processed per day. This valuable data is integrated directly into THREADS.” The power of THREADS for law enforcement is the aggregation of data from facilities across the “nationwide

targets ‘working group.’ For example, an inmate may call his brother every Tuesday, and then right after that phone conversation he calls his cousin. THREADS will highlight this call pattern implying to the investigators that whatever was discussed with the brother, most likely was discussed with his cousin.”).

⁵⁶ FCC Ex Parte Submission, WC Docket No. 17-126, ITC-T/C-20170511-00094, ITC-T/C-20170511-00095, at 24 (Aug. 2, 2017).

community”.⁵⁷

74. To create this “community,” Securus formally asked its correction facility customers to opt in to sharing their facility’s data. In return, Securus promised access to a broad suite of analytics and data.

75. Securus intended that THREADS would “bridg[e] the gap between Corrections and Law Enforcement,” by giving law enforcement access to all the data that resided on the Securus Call Platform nationwide.⁵⁸

76. This data, then, includes such varied streams as the content of billions of personal calls, video visitation data, financial information, biometric data, and location data. More than half of the unique individuals whose information has been collected in this system were *not* incarcerated when the data was collected.⁵⁹

77. DOC has THREADS and allows Securus to feed not only its call data, but also Securus-provided tablet data and a Securus-subsiary’s money transfer service data for adding money to a commissary account into its THREADS system.

E. DOC Benefits from the Securus Relationship

78. While each of Securus’s data collection streams (voiceprint, location data, and national aggregation through THREADS) produces eye-swimming quantities of data, Securus provides the products to collect this data free of financial charge to its law enforcement customers.

79. DOC receives both THREADS and continuous voice verification at no additional financial cost, for example.⁶⁰ Instead, DOC offers and Securus receives something far more

⁵⁷ *Id.* at 21, 24, 30.

⁵⁸ *Id.* at 25.

⁵⁹ *Id.* at 24.

⁶⁰ *See* Amendment No. 5 to the Agreement Between DOC and Securus, signed Jan. 17, 2023, Exhibit 1; Securus, *BAFO*, at 2, 4.

valuable in return for DOC's access to these tools: New Yorkers' personal data, including biometric, associational, and financial data.

80. Securus's business model—driven by technology development based in machine learning—values access to this data over financial compensation. This is because machine learning algorithms (like Securus's voice verification system for example) rely on access to extensive, non-public datasets (*e.g.*, massive amounts of call voice recordings) to hone and train their (*e.g.*, voice recognition) algorithms. This data is necessary to develop and then to improve their products.

81. While DOC specifically “retains sole ownership and intellectual property rights in and to all information, data (call records and recordings), data compilations, reports, charts, graphs, diagrams, or other information provided or made accessible by the DOC to [Securus], or created by [Securus] pursuant to the Agreement” under its contract with Securus, the contract specifically permits use of “general knowledge, skills, . . . techniques . . . learned . . . during the performance of . . . obligations under the Agreement.”⁶¹ In a machine learning world, the Use of General Knowledge clause gives Securus the ability to profit from access to DOC data, while allowing DOC to appear to retain data ownership.

82. Thus, even after Securus stopped paying DOC a commission, originally guaranteed at a minimum of \$5 million a year, in 2019,⁶² Securus continued to compensate DOC for its access to New Yorkers' data through providing it with no-cost technology add-ons, like continuous voice verification. And the manpower, equipment, and services DOC had been receiving without financial charge continued unchanged.

⁶¹ DOC-Securus Contract, §§ 7.2, 7.3.

⁶² Amendment No. 3 to the Agreement Between DOC and Securus, entered into May 1, 2019.

83. What's more, Securus also offers no-cost technology add-ons to its services that reduce DOC expenses and staffing needs. For example, in its initial RFPs for the Inmate Phone System, DOC reflected that the new phone system would result in "expense savings" by eliminating the need for consultants and services which had been necessary to maintain its legacy phone system.⁶³ Instead, DOC ultimately received from Securus at least two full-time, onsite administrators/technicians, along with more than 1,800 pieces of technical equipment and 24-hour service, without spending a dime.⁶⁴

F. DOC's Purpose in Building a Community Surveillance System Is Not Tethered to Maintaining Internal Jail Security

84. Even before BOC accepted DOC's proposed change to the prohibition on listening to and monitoring phone calls without a warrant, community members, BOC members, and legal professionals repeatedly voiced concerns about the erosion of civil rights and liberties and the attorney-client relationship.⁶⁵

85. Attorneys warned that DOC had not explained how listening and monitoring would be technically carried out, cautioning that without this detail this change would inevitably lead to an unprincipled and unjustified system of universal surveillance.⁶⁶

86. DOC acknowledged that it was making its request at a time when crime was at an all-time low, custody levels were lower than they had been in a decade, and security incidents were down. DOC justified its request by arguing that the "minimum standards dating to 1978

⁶³ DOC, *Request for Proposal for the Inmate Phone System*, at 4.

⁶⁴ Securus, *BAFO*, at 2-3.

⁶⁵ See BOC, *Public Hearing on Proposed Amendments to Minimum Standards to NYC Correctional Facilities* (Apr. 17, 2007); BOC, *Meeting Minutes* (May 10, 2007); BOC, *Public Hearing on Proposed Amendments to Minimum Standards to NYC Correctional Facilities* (June 14, 2007); BOC, *Meeting Minutes* (Nov. 8, 2007).

⁶⁶ See, e.g., BOC, *Public Hearing on Proposed Amendments to Minimum Standards to NYC Correctional Facilities*, Testimony of Corey Stoughton of the NYCLU (Apr. 17, 2007).

shackle us in our attempt to run safe jails in ways no other jail in the State of New York is restrained.” DOC expressly tied its need for the rule change to its appetite for intelligence gathering.⁶⁷

87. DOC began its surveillance project slowly, with then-Commissioner Horn reporting that “only about five staff members are authorized to listen to calls, and DOC has an internal ‘warrant’ process whereby listening has to be based upon a written justification that ultimately is reviewable.”⁶⁸

88. Even prior to the standards change, and as early as 2007, the NYPD began trying to obtain intelligence from Rikers Island, executing a Memorandum of Understanding (“MOU”) between DOC and the NYPD, as well as the Department of Probation. The 2007 MOU’s stated objective was to: “share certain information electronically for the benefit of the public, to enhance public safety, secure facilities and detention centers, to aid in the detection, investigation, and prevention of criminal activity, to aid in the rehabilitation of incarcerated or supervised persons, and to support law enforcement activities.”⁶⁹ This information specifically included DOC’s phone and visitor data.

89. By 2009, the NYPD had taken the intelligence relationship further, establishing a presence on Rikers Island at a new information-sharing hub: the Rikers Island Fusion Center.⁷⁰

⁶⁷ *Id.*, Testimony of DOC Commissioner Martin Horn.

⁶⁸ BOC, *Meeting Minutes* (Sept. 11, 2008).

⁶⁹ Memorandum of Understanding Between New York City Police Department and New York City Department of Correction (Oct. 24, 2007).

⁷⁰ See @CorrectionsNYC, Twitter (Oct. 30, 2018, 3:25pm),

90. United States Department of Homeland Security created Fusion Centers to serve as network access points for the different law enforcement agencies operating in a jurisdiction: local, state, and national. Various law enforcement entities sit in common space within a fusion center and share database access credentials with each other. For New York City jails that is—at least—DOC, the NYPD, and federal law enforcement agencies.

91. In 2014, when Securus presented its BAFO to DOC, the company touted its relationship to NYPD, flagging that the police department *already* had a THREADS subscription even prior to DOC’s adoption of Securus’s system.⁷¹

92. Given the entrenched intelligence relationship between DOC and NYPD, Securus’s marketing angle made sound business sense. In the New York City environment, DOC’s political motivation was to “obtain intelligence information,” “provid[ing] a benefit to other law enforcement agencies.”⁷²

93. At present, it is clear that the NYPD has a dedicated team of officers, detectives,



<https://twitter.com/CorrectionNYC/status/1057352758087598081> ;

New York City Council, *Hearing of the Committee on Criminal Justice*, Testimony of Commission Cynthia Brann (March 14, 2019), <https://www.nyc.gov/site/doc/media/march-14-testimony.page>. The only other traces of the Rikers Island Fusion Center’s existence come from NYPD police reports received in criminal discovery, and periodic social media mentions by staff. Its exact origin, purpose, or founding date are not publicly disclosed.

⁷¹ Securus, *BAFO*, at 3.

⁷² DOC, Operations Order: *Inmate Telephone Recording & Monitoring*, § II, effective June 10, 2016.

and staff from its Real Time Crime Center who specifically form the “Rikers Fusion Team.” Based on references in DOC’s post-breach disclosures and discovery received in criminal cases, this Rikers Fusion Team appears to have direct access to Securus’s NextGen Secure Communications Platform and all its data streams.

94. Brooklyn Defenders learned through a Freedom of Information Law request to DOC in 2022 that DOC was recording almost 25,000 phone calls per day. However, DOC itself was listening to less than 2 percent of those calls. DOC could provide no information or statistics about whether or how the use of those call recordings had enhanced internal security.⁷³

95. The Department’s rationale for creating a universal surveillance system, therefore, was always only tangentially related to internal security. Instead, as DOC made clear in its initial Request for Proposal and in its vendor selection, DOC’s surveillance apparatus was intended to be community facing.

96. Securus readily obliged DOC’s desired focus for the project, as it also aligned with the company’s product development strategy and philosophy.

97. For example, Securus is designing its ranking analytics and processing algorithms to target the associational ties of people both within and outside carceral facilities. A 2010 patent application explains Securus’s intention to equip an “investigator” to “identify known or suspected gang members and then link those gang members to their visitors, to individuals who provide funds to the gang members, to individuals who communicate with the gang members and to gang members who communicate with certain individuals.”⁷⁴

98. While Securus’s focus on gang enforcement may seem tethered to facility internal

⁷³ Ltr. from DOC Record Access Officer to Elizabeth Vasquez, re: DOC Initial Response to FOIL 22FR1426, May 24, 2022.

⁷⁴ U.S. Patent No. 7,805,457 B1 (filed Sept. 28, 2010).

security, Securus went further, clarifying: “As used herein, the terms gang and security threat group are used broadly and are intended to include any known or suspected criminal, political, anti-social, anti-government, or terrorist organizations or groups of any size, including groups having local, national, and/or international members and/or having centralized, decentralized, formal or informal management and control.”⁷⁵ This definition of Securus’s associational purpose is so broad as to be meaningless, and instead reveals the company and its customers’ appetite for suspicionless mass surveillance of the community.

99. However, Securus (and, by extension, its customers) have gone even further in revealing the full contours of their project. Securus submitted a 2022 patent entitled, “Rewards for Non-Residents Associated with Controlled-Environment Facility Residents.” In this patent, Securus outlined a system for providing people who were *not* incarcerated with rewards, such as preferential calling, for “good behaviors related to electronic communications with” those incarcerated.⁷⁶ Securus, through this patent, revealed an intention to monitor and control the behavior not merely of those subject to formal criminal suspicion and legal process, but more critically the behavior of people who are not incarcerated but who communicate with or are connected to those detained.

100. Securus and those who contract with it, like DOC, have orchestrated a broad system of social control in collaboration with law enforcement, despite the utter lack of notice, provision of rights, or prerequisite of reasonable suspicion, probable cause, or guilt beyond a reasonable doubt of any legal offense. Instead, Securus and its customers envision a world where associational and speech-based rights are technologically monitored, limited, and controlled for

⁷⁵ *Id.* (emphasis added).

⁷⁶ U.S. Patent No. 11,461,800 B1 (filed Oct. 4, 2022).

certain members of our community.


101. Securus's prison and jail surveillance products are thus not merely (or even primarily) about ensuring internal facility security, but rather are designed to expand the community-based information and social networks available to law enforcement without court oversight, warrant requirements, or regulation.

102. Outside of the carceral environment, none of this information would be available to law enforcement without an articulable suspicion and legal process. Securus's products and DOC's use of them turn our Fourth and First Amendment paradigms on their head.

103. What's more, because Securus's products cast their community nets outward from New York City jails, the Securus/DOC surveillance program reflects the racist targeting of Black and Brown communities documented within the criminal legal system at large. Perhaps even more sinisterly, this system constructs its net out of community association itself, generating data directly from *communication*, the lifeblood of relationship and community.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: April 15, 2024
Brooklyn, New York



Elizabeth Daniel Vasquez