epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL COMMUNICATIONS COMMISSION

Request for Comment on Securus Technologies, LLC's Petition for Waiver of the Inmate Calling Services Per-Minute Rate Requirement, WC Docket No. 12-375

86 Fed. Reg. 70427

January 7, 2022

---

In response to the request for comment on the petition by Securus Technologies, LLC ("Securus") for waiver of the inmate calling services per-minute rate requirement, published on October 10, 2021, by the Federal Communications Commission ("the Commission"),[1] the Electronic Privacy Information Center ("EPIC") submits the following comment on Securus' petition and Worth Rises' concerns raised in response to Securus' petition. EPIC joined Worth Rises latest comment on this docket,[2] and writes separately here to underscore the serious and systemic failures of Securus Technologies. EPIC urges the Commission to subject any petition from Securus to the highest levels of scrutiny and to act aggressively to protect the vulnerable populations that make up Securus's client base from unfair pricing, surveillance, and fraud.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values.[3] EPIC has filed amicus briefs on attorney-client

[1] 86 Fed. Reg. 70427, https://www.govinfo.gov/content/pkg/FR-2021-12-10/pdf/2021-26586.pdf.
[2] See comments of Worth Rises, EPIC, et al. also filed in this docket.
[3] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

privilege and petitioned the FCC for rulemaking regarding the privacy and security of phone subscriber data, as well as offered congressional testimony on the same issues.[4]

Securus has a long track record of harming inmates, their families, and their lawyers. Securus has been caught violating attorney-client privilege,[5] allowing improper access to Customer Proprietary Network Information (CPNI) (including location data),[6] misleading regulators,[7] deceiving consumers,[8] and exploiting vulnerable populations.[9] In light of Securus' track record, EPIC recommends that the Commission view Securus' claims in the most skeptical light and subject

[4] *See, e.g.,* Br. of Amici Curiae Electronic Privacy Information Center (EPIC) in Support of Appellant, Anibowei v. Wolf, No. 20-10059 (June 9, 2020), https://epic.org/documents/anibowei-v-wolf/ (amicus in support of plaintiff, an attorney whose phone was searched without a warrant by border agents at Dallas airport); Report and Order and Further Notice of Proposed Rulemaking, Federal Communications Commission, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Information, FCC 07-22 (Apr. 2, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf (Commission Report and Order on protecting Customer Proprietary Network Information (CPNI) initiated by EPIC petition); EPIC Letter to House Energy & Commerce Committee, Accountability and Oversight of the Federal Communications Commission (May 14, 2019), https://epic.org/documents/accountability-and-oversight-of-the-federal-communications-commission/ (testimony regarding the FCC's oversight of robocalls, location tracking, and unnecessary collection and retention of subscriber call records).

[5] Jordan Smith & 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/.

[6] AT&T Inc., Notice of Apparent Liability, File No.: EB-TCD-18-00027704 (2020), at ¶¶ 20, 51, 54, 60, https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf (describing officer's misuse of location data permitted by Securus) [AT&T NAL].

[7] *Securus Tech. Inc.*, Consent Decree, 32 FCC Rcd 9552 (11) ( 2017), https://www.fcc.gov/document/securus-agrees-pay-17-million-civil-penalty; Peter Wagner, *Uncovering Securus' Profits*, Prison Policy Initiative (Jun. 19, 2015), https://www.prisonpolicy.org/blog/2015/06/19/securus-profits/ (identifying discrepancy between profits reported to regulators and profits reported to investors).

[8] *In the Matter of Rates for Interstate Inmate Calling Services*, Letter to Securus Technologies from Matthew S. DelNero, WC Docket No. 12-375 at 1 (Dec. 3, 2015), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1203/DA-15-1382A1.pdf (letter from Chief of Wireline Competition Bureau to Securus regarding Securus' inaccurate and misleading statements regarding mandatory fees); *In the Matter of Rates for Interstate Inmate Calling Services*, Reply Comments of Prison Policy Initiative, Inc. on Fifth Further NPRM, WC Docket No. 12-375 at 5-7 (Dec. 17, 2021), https://ecfsapi.fcc.gov/file/12171576121872/2021-12-17%20-%20PPI%20Reply%20Comments%20on%205th%20FNPRM.pdf (describing Securus' misleading phone menu as an unjust and/or unreasonable practice).

[9] Peter Wagner and Alexi Jones, *State of Phone Justice: Local jails, state prisons and private phone providers*, Prison Policy Initiative (Feb. 2019), https://www.prisonpolicy.org/phones/state_of_phone_justice.html (noting in Feb. 2019 that WesternUnion and Moneygram charge more than $11 each to send $25 to Securus, collected in part on behalf of the provider, even calling it a "revenue share" in some instances, in contravention of the FCC's regulation); Hannah Kozlowska, *Prison communications company Securus will no longer require jails to ban in-person visits*, Quartz (May 9, 2015), https://qz.com/400055/prison-communications-company-securus-will-no-longer-require-jails-to-ban-in-person-visits/ (Securus abandoning practice of requiring jails that use its video calling service ban in-person visits).

their claims to the greatest scrutiny, as the company has repeatedly demonstrated its proficiency in exploiting vulnerable people and regulatory loopholes.

In 2015, a white-hat hack of Securus' phone records database revealed that the company had left 70 million recorded calls vulnerable to breach, and that the company retained records of over 14,000 calls between prisoners and their attorneys.[10] David Fathi of the ACLU's National Prison Project called Securus' actions possibly "the most massive breach of the attorney-client privilege in modern US history."[11] Since 2015, Securus has settled several lawsuits for improperly recording privileged attorney-client calls after the clients specifically designated them as such.[12] Securus' violations of attorney-client privilege continued for most of the last decade, and may be ongoing.[13]

Securus does not just exploit its own call records, but harvests and sells the location data of individuals calling in to prisons. In 2018, Senator Ron Wyden revealed that Securus serves as a data broker purchasing location data from cell providers and selling that information to the government, effectively skirting the warrant requirement of the Fourth Amendment. In a letter to the Commission, Sen. Wyden described Securus' provision of data to government agencies as "needlessly expos[ing]

---

[10] Jordan Smith & 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/.

[11] *Id*. (David Fathi, Director of ACLU's National Prison Project, went on to say "A lot of prisoner rights are limited because of their conviction and incarceration, but their protection by the attorney-client privilege is not.")

[12] Jordan Smith, *Securus Settles Lawsuit Alleging Improper Recording of Privileged Inmate Calls*, The Intercept (Mar. 16, 2016), https://theintercept.com/2016/03/16/securus-settles-lawsuit-alleging-improper-recording-of-privileged-inmate-calls/ (Securus settled in Austin in 2016), Dan Margolies, *Leavenworth Inmates Reach $1.45 Million Settlement Over Taped Attorney-Client Phone Calls*, NPR News ( https://www.kcur.org/news/2019-08-26/leavenworth-inmates-reach-1-45-million-settlement-over-taped-attorney-client-phone-calls (Securus and the prison services provider Civic Core allegedly continued recording attorney-client calls even after a District Court ordered the prison to immediately halt the practice).

[13] Ella Fassler, *Prison Phone Companies Are Recording Attorney-Client Calls Across the US*, Vice News (Dec. 13, 2021), https://www.vice.com/en/article/7kbbey/prison-phone-companies-are-recording-attorney-client-calls-across-the-us (noting violations occurring in 2019, and linking to lawsuits against Securus for similar behavior in seven states); Kerry Maeve Sheehan, *Securus Leak of Prison Call Records Underscores Importance of FCC Oversight*, Public Knowledge (Dec. 8, 2015), https://publicknowledge.org/securus-leak-of-prison-call-records-underscores-importance-of-fcc-oversight/ ("Systems like Securus' must be designed to allow the monitoring of information that is *not* privileged and confidential, and the safeguarding of the information that *is*.", "Once the data has been reviewed and there's no lawful need to maintain the information, there should be a process for purging that data from the database. The obligation that providers cooperate with law enforcement does not provide an absolute right to use or allow blanket access to customers' metadata, even when those customers are imprisoned.").

millions of Americans to potential abuse and surveillance by the government"[14], providing real-time location data "to the government for nothing more than the legal equivalent of a pinky promise."[15] Rep. Doyle characterized Securus' service offerings, as revealed by Sen. Wyden's investigation, as "forc[ing] families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family members. This seems like no choice at all."[16]

In a more recent review of Securus' location data practices, Commissioner Starks described the company as a wrongdoer that has "behaved outrageously."[17] Securus was a downstream purchaser of phone subscriber location data, making that sensitive data available to law enforcement without verifying the legitimacy of their requests. One law enforcement officer, Sheriff Cory Hutcheson personally obtained customer location data without authorization more than 2,000 times using Securus' service, revealing phone location data each time. [18] Victims were not limited to the family and friends of prisoners, but extended to highway patrol officers and a judge.[19] Securus disclosed the records to Sheriff Hutcheson without even reviewing the supporting documentation he

[14] Senator Ron Wyden, Letter to FCC Chairman Ajit Pai (May 28, 2018), https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-fcc.pdf.
[15] *Id*. The Electronic Frontier Foundation also characterized these Securus practices as woefully inadequate: "it doesn't matter what a Securus customer uploads to the web portal—it could be a cat video for all we know—they will still get access to the real-time location data of the target of their inquiry by checking the box—without any consequences or accountability for misuse." Stephanie Lacambra & Jennifer Lynch, *Senator Wyden Demands Answers from Prison Phone Service Caught Sharing Cellphone Location Data*, EFF.org (May 11, 2018), https://www.eff.org/deeplinks/2018/05/senator-wyden-calls-fcc-investigate-real-time-location-data-sharing-all-cellphone.
[16] Doyle Remarks at Communications Privacy Hearing, House Committee on Energy and Commerce (Jul. 11, 2018), https://energycommerce.house.gov/newsroom/press-releases/doyle-remarks-at-communications-privacy-hearing ("At least one company, Securus, used their access to this data to create a service for tracking and locating nearly every cell phone in real time. On top of that Securus forced families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family member. That seems like no choice at all.")
[17] AT&T NAL, *supra* note 6, Statement of Commissioner Geoffrey Starks, at 40-41, https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf ("[O]ur action today is limited to the major wireless carriers. But we know from this investigation that they are not the only wrongdoers. Securus, for one example, behaved outrageously.") Despite both Commissioner Starks' comments and Sen. Wyden's letter, the Commission only announced an investigation into LocationSmart, the aggregator from whom Securus purchased the data. Press Release, *Wyden Praises FCC Decision to Investigate Flaw Allowing Real-Time Tracking of Millions of Americans* (May 18, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-praises-fcc-decision-to-investigate-flaw-allowing-real-time-tracking-of-millions-of-americans.
[18] AT&T NAL at 40.
[19] *Id*.

submitted to justify the searches, which was often wholly irrelevant.[20] And Hutcheson was likely not the only one paying Securus for phone subscriber's location information. Bounty hunters, citizens, stalkers, and criminals could use this data to surveil individuals without their knowledge.[21]

In October 2015, then-Commissioner Rosenworcel noted the "staggering statistics" and "sky-high cost" surrounding incarceration in the United States.[22] Chairwoman Rosenworcel observed that "[t]his challenge is well beyond the authority of this Commission" but that "there is also something the Commission can do."[23] While the FCC may not be able to wholly remedy the epidemic of overcharging for services in the prison system, the Commission does have the jurisdiction to prevent exploitative prison phone practices and protect prisoners and their communities from surveillance. EPIC recommends the Commission do what it can here to prevent further abuse and exploitation of a particularly vulnerable population.

**Conclusion**

EPIC urges the Commission to treat Securus' petition with the utmost skepticism. Even where the company had the opportunity to turn a new leaf, its exploitative practices continued. Securus has demonstrated time and again that the company views prisons and the government, not incarcerated persons and their communities, as its true customers. The FCC can and should act to correct abusive surveillance practices and to ensure that prisoners and their families pay a fair rate calling services. As Chairwoman Rosenworcel urged in this very docket when she was a

[20] *Id.*
[21] *See*, Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Vice News (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile ("The investigation also shows that a wide variety of companies can access cell phone location data, and that the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data.")
[22] Statement of Commissioner Jessica Rosenworcel Re: Rates for Interstate Inmate Calling Services, WC Docket No. 12-375, https://docs.fcc.gov/public/attachments/DOC-335984A4.pdf.
[23] *Id*. Then-Commissioner Rosenworcel went on to address the outrageous rates paid by families of prison inmates. *Id.*

Commissioner, the Commission should take what actions it can to address the staggering growth and burdensome costs of our prison system.

Respectfully submitted,

/s/ Alan Butler
Alan Butler
Executive Director

/s/ Jake Wiener
Jake Wiener
Law Fellow

/s/ Chris Frascella
Chris Frascella
Law Fellow