Largest Detention Communications Companies

The two largest detention facilities communications companies are Global Tel*Link (GTL) and Securus Technologies. According to an analysis performed by the Prison Policy Initiative, as of 2018, GTL and Securus accounted for about 83% of the market, with GTL occupying 43% of the market and Securus occupying 40% of the market.[1]

Global Tel Link (GTL):

GTL is a Virginia-based detention communications company that contracts with 2,300 facilities in 50 states.[2] According to GTL's website, 1.6 million incarcerated persons—or 74% of incarcerated persons in the U.S.—use its services.[3] GTL provides correctional facilities with a web-based telephone platform, which records and stores calls made to and from detention facilities, tablets detainees can use to read e-books and make phone and video calls, and other services. GTL also operates a lab that extracts "digital evidence" from digital devices seized in detention facilities. This evidence is used to "stop and solve crimes."[4]

i. Media coverage

Most of the media coverage of GTL has related to the exorbitant rates detainees must pay in order to make phone calls. In the past few years, however, GTL has received a fair amount of media coverage related to privacy issues. In 2018, the company came under fire when it came to light that 34,000 calls between Orange County incarcerated persons and their attorneys were illegally recorded.[5] An Orange County Grand Jury report published afterwards determined that several of the calls had been accessed, and that some information from these calls was provided to the county's District Attorney.[6] GTL has since acknowledged that something similar occurred in two Florida counties in 2014.[7]

ii. Litigation

There has not been very much media coverage of privacy-related litigation against GTL, but at least one lawsuit was filed after GTL's recording of attorney-client communications in Orange

---

[1] Petition to Deny, In re TKC Holdings Inc., WC Docket 18-193 (FCC July 16, 2018).
[2] *GTL Leadership By the Numbers*, GTL, https://www.gtl.net/about-us/gtl_by_the_numbers/ (last visited May 18, 2020).
[3] *Id.*
[4] *Stopping Crime Before It Happens – Intelligence Tools, Analysts Prevent Planned Attacks*, GTL, https://www.gtl.net/about-us/press-and-news/stopping_crime_before_it_happens_intelligence_tools_analysts_prevent_planned_attacks/ (last visited May 18, 2020).
[5] Todd Harmonson, *Nearly 34,000 Orange County Inmates' Calls to Attorneys Recorded, Not the 1,079 Originally Reported*, https://www.ocregister.com/2018/11/09/nearly-34000-orange-county-inmates-calls-to-attorneys-recorded-not-the-1079-originally-reported/ (last visited May 18, 2020).
[6] Elizabeth Weill-Greenberg, *'Do Not Record'*, https://theappeal.org/do-not-record-orange-county-jail-phone-recordings/ (last visited May 18, 2020).
[7] L.A. Times Editorial Board, *Editorial: Attorney-Client Communications in Jail are Supposed to be Confidential. They're Not*, L.A. TIMES (Sep. 11, 2018, 4:05 AM), https://www.latimes.com/opinion/editorials/la-ed-eavesdropping-20180911-story.html.

County. In 2019, a group of detainees and attorneys filed a class action lawsuit seeking $500 million in damages, $5,000 for each recorded attorney-client call.[8] The lawsuit appears to be ongoing.

iii. Cases

1. **Case caption:** Mark Moon v. County of Orange et al
   Docket No: 8:19-cv-00258

Securus Technologies:

Securus is a Dallas-based detention communications company. Its phone system allows prisons and jails to monitor and record both placed and received calls and then store them. As of 2015, the company purported to contract with 1,900 correctional facilities, and their database included over 100 million call records.[9] Recently, the company has developed an app that allows users to conduct video calls and send photos, e-cards, and short video messages.[10]

i. Media coverage

Like GTL, most media coverage of Securus involves the cost of making calls from detention facilities. However, Securus has also received a substantial amount of privacy and Sixth Amendment-related media coverage.

For example, a 2015 security breach of Securus's records received extensive media coverage. The breach allowed a hacker to access 70 million phone calls, which involved prisoners in 27 different states.[11] According to the Intercept, the records included "prisoners' first and last names; the phone numbers they called; the date, time, and duration of the calls; the inmates' Securus account numbers" and links allowing recordings of the calls to be downloaded. The hacked records included at least 14,000 recorded conversations between attorneys and their incarcerated clients, despite the fact that Securus had stated that it did not record these phone calls.[12] Securus's system was also breached in 2014, when a hacker gained access to three of former NFL player Aaron Hernandez's personal phone calls while he was awaiting trial.[13]

In 2017 and 2018, Securus also received media attention for privacy related issues when it came to light that the system could be used to "find the whereabouts of almost any cellphone in the country within seconds," and that it was not properly vetting surveillance requests from customers.[14] The New York Times reported that criminal justice actors were using the service to

---

[8] Scott Schwebke, *Lawsuit seeks $500 million in Orange County Jail Phone Scandal*, THE ORANGE COUNTY REGISTER (April 4, 2019 at 6:47 PM), https://www.ocregister.com/2019/04/04/lawsuit-seeks-500-million-in-orange-county-jail-phone-scandal/.

[9] Jordan Smith & Micah Lee, *Not So Securus*, THE INTERCEPT (November 11 2015, 11:43 AM), https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/.

[10] SECURUS TECHNOLOGIES, https://securustech.net/ (last visited May, 18 2020).

[11] Smith, *supra*, note 9.

[12] *Id.*

[13] *Id.*

[14] Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (MAY 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

track peoples' location without court orders.[15] For example, one official used Securus to track down a woman who left a drug rehab center before she was supposed to.[16] Another report from 2018 drew attention to the fact that the system could be used to obtain and share the cellphone information of anyone who was called by an individual in a detention facility that contracted with Securus.[17]

In 2019, Securus's voice recognition technology also received some media coverage. The technology "extract[s] and digitize[s] the voices of incarcerated people into unique biometric signatures, known as voice prints."[18] The voice prints are then added to a database that can be used to search for other calls made by that individual.[19] According to the Intercept, the technology can also mine outside parties' voiceprints.[20] This allows investigators to track '"suspicious activities," such as "multiple inmates speaking to one person on the outside on a reoccurring basis.'"[21] There has also been some media coverage of privacy litigation that Securus has been involved in, which I've outlined below.

ii. Litigation

The two privacy-related lawsuits that have received the most media attention were brought by groups in Kansas and Austin.

Austin lawsuit:

In 2014, the Austin Lawyers Guild, the Prison Justice League and several defense attorneys filed a class action lawsuit against Securus and the Travis County DA and Sheriff's office alleging that Securus recorded privileged phone conversations between incarcerated persons and their attorneys, and that prosecutors later accessed and listened to these recordings.[22] The plaintiffs requested that the judge declare the practice unlawful, enjoin the defendants from continuing to record, disclose, and use these communications, and order the defendants to destroy all unlawfully recorded attorney-client communications.[23] The case settled in 2016.[24]

---

[15] *Id.*
[16] *Id.*
[17] Neema Singh Guliani & Nathan Freed Wessler, *Company That Handles Prison Phone Calls Is Surveilling People Who Aren't in Prison*, ACLU BLOG (May 11, 2018, 10:00 AM), https://www.aclu.org/blog/privacy-technology/location-tracking/company-handles-prison-phone-calls-surveilling-people-who.
[18] George Joseph & Debbie Nathan, *Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints*, The Intercept (Jan. 230, 2019, 10:00 AM), https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus//.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Jordan Smith, *Securus Settles Lawsuit Alleging Improper Recording of Privileged Inmate Calls*, THE INTERCEPT (Mar. 16, 2016, 11:03 AM), https://theintercept.com/2016/03/16/securus-settles-lawsuit-alleging-improper-recording-of-privileged-inmate-calls/.
[23] Complaint, Austin Lawyers Guild v. Securus Techs, Inc., No. 1:14-cv-00366-LY (W.D. Tex. July 23, 2014).
[24] Smith, *supra* note 22.

Kansas lawsuits:

In 2017, two lawsuits were filed against Securus and Leavenworth Detention Center's operator—CoreCivic. They alleged that the defendants had improperly recorded privileged attorney-client communications in violation of state and federal wiretap laws. One lawsuit was filed by former detainees at Leavenworth and the other by two attorneys with clients at Leavenworth.[25] Discovery revealed that more than 1,300 phone calls between public defenders and their clients had been recorded, and the U.S. Attorney's office acknowledged that prosecutors had listened to some of the recorded calls.[26] The case filed by detainees turned into a class action lawsuit, which ultimately reached a settlement agreement requiring Securus to pay $350,000.[27] The case filed by the attorneys appears to still be ongoing.

iii. Cases

1. **Citation:** Romero v. Securus Techs., Inc., 331 F.R.D. 391 (S.D. Cal. 2018).
   Case No: 16cv1283 JM (MDD)

2. **Citation:** Hernandez v. Securus Techs., Inc., No. CV 16-12402-RGS, 2017 WL 826915 (D. Mass. Mar. 2, 2017).
   Case No: 16-12402-RGS

3. **Citation:** Johnson v. CoreCivic, No. 4:16-CV-00947-SRB, 2018 WL 7918162 (W.D. Mo. Sept. 18, 2018)
   Case No: 4:16-cv-00947-SRB

4. **Citation:** Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042 (D. Kan. Mar. 5, 2018)
   Case No: 17-2320-JAR-JPO

5. **Citation:** Guild v. Securus Techs., Inc., No. 1:14-CV-366-LY, 2015 WL 10818584 (W.D. Tex. Feb. 4, 2015).
   Case No: 1:14-CV-366-LY

Zoom:

The use of Zoom for attorney-client communications, along with concerns about the security of the platform, has increased substantially over the past few months. The increased use of the platform has raised a number of ethical concerns about how to maintain attorney-client privilege and keep client information private more broadly.

---

[25] Dan Margolies, *Bombshell In Leavenworth Tapings Case: 1,300 Public Defender Calls Recorded Over Two Years*, KCUR (June 6, 2018, 9:20 AM), https://www.kcur.org/news/2018-06-06/bombshell-in-leavenworth-tapings-case-1-300-public-defender-calls-recorded-over-two-years.
[26] *Id.*
[27] *Id.*

i. Ethical Uses of Technology:

Federal Guidance:

The ABA's Model Rules impose general requirements on attorneys who use digital technology to communicate confidential or privileged information. Rule 1.1, Comment 8, requires that attorneys "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…."[28] Most states have adopted the language of this rule or similar language into their own ethical codes. Furthermore, under Rule 1.6, lawyers are required to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[29] What constitutes "reasonable efforts" is not specifically defined. Instead, whether efforts are reasonable depends on a number of nonexclusive factors that include "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients."[30]

In Formal Opinion 477, the ABA offered a number of considerations attorneys should take into account when deciding what type of security client information and communications warrant.[31] Numbers one, two, three, four, and seven are particularly relevant in the Zoom context. Number one is to "understand the nature of the threat."[32] This means evaluating both the nature of the client information at risk as well as the risk of "intrusion" into the matter.[33] Higher risk scenarios require greater efforts to protect client information and communications.[34] The second is to "understand how client confidential information is transmitted and where it is stored," so as to better understand how it could land in the hands of unauthorized parties.[35] The third is to "understand and use reasonable security measures."[36] This requires that lawyers understand how to take steps to protect client information, such as creating appropriate passwords, updating software, and encrypting sensitive client information.[37] The fourth is to "determine how electronic communications about client matters should be protected."[38] For example, attorneys should know when the sensitive nature of information makes password-protection or encryption appropriate.[39] Importantly in this particular context, "lawyers should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party," since privilege and confidentiality could be waived.[40] Finally, the seventh is that attorneys should "conduct due diligence on vendors providing

---

[28] Model Rules of Prof'l Conduct, r. 1.1 cmt. 8 (Am. Bar Ass'n 1983).
[29] Model Rules of Prof'l Conduct, r. 1.6(c) (Am. Bar Ass'n 1983).
[30] Model Rules of Prof'l Conduct, r. 1.6(c) cmt. 18 (Am. Bar Ass'n 1983).
[31] *See* ABA Comm'n on Prof'l Ethics & Prof'l Responsibility, Formal Op. 477R (2017).
[32] *Id.* at 5.
[33] *Id.*
[34] *Id.*
[35] *Id.* at 6.
[36] *Id.*
[37] *Id.*
[38] *Id.* at 7.
[39] *Id.*
[40] *Id.*

communication technology," which means evaluating whether or not the safeguards that a particular platform employs are sufficient.[41]

State Guidance:

State guidance on ethics and technology have come from two primary sources: state supreme courts and state bar associations.

State Supreme Court orders: Most state supreme courts have issued orders relating to court operations during Covid. In most cases, these orders include information related to conducting remote trials, but they don't contain anything about videoconferencing or Zoom outside of the trial context.

State Bar Association opinions: Pennsylvania is the only state bar association that I could find that has issued a relevant ethics opinion.[42] Titled "Ethical Obligations for Lawyers Working Remotely," the opinion deals mostly with how to maintain confidentiality via electronic communications platforms generally, but it does not mention Zoom specifically.[43]

State Bar Association websites: Some state bar associations have articles and blog posts on their website related to Zoom and confidentiality, but these were mostly written by in-state lawyers and not the Bar Association itself. The information and advice they include is summarized below.

ii. Application in the Zoom context

Given these considerations, there are a number of steps attorneys can take in the Zoom context to prevent the disclosure of attorney-client communications. First, attorneys can create password-protected meetings and use settings to prevent participants from being able to record the meeting or share their screens.[44] They can also create "Waiting Rooms," which allow the host of the meeting to admit meeting participants individually. The meeting can then be locked once all participants have been admitted.[45] Additionally, attorneys should probably refrain from recording conversations with clients. These recordings can be stored by Zoom, which not only opens the door to the potential waiver of attorney-client privilege, but could also potentially lead to that recording being subpoenaed or shared.[46]

Attorneys may also want to gain a general sense of the type of security problems that Zoom users have encountered and whether or not Zoom has fixed these problems. For example, in March, after it came to light that Zoom was sharing user data with Facebook, Zoom removed

---

[41] *Id.* at 9.
[42] P.A. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Op. 2020-300 (2020).
[43] *Id.*
[44] David Saunders & David Greenwald, *INSIGHT: Zooming and Attorney-Client Privilege*, BLOOMBERG LAW (May 22, 2020, 3:01 AM), https://www.bloomberglaw.com/document/XFII4528000000?bna_news_filter=us-law-week&jcsearch=BNA%252000000171ea1cd000a97fea7e90ac0001#jcite.
[45] *Id.*
[46] *Id.*

this feature from platform.[47] Similarly, after hundreds of reports of "Zoombombing," the company enabled the "waiting rooms" feature and made password protection possible for all calls.[48] But there are other potential security problems with the app that the company has not resolved. First, although the company purported to use end to end encryption in its marketing materials, in late March, a report by the Intercept revealed that it did not.[49] In April, Zoom bought security company Keybase in order to develop this feature,[50] but it has not announced when the feature will be available. Second, in April, a research firm identified a bug in the platform that could allow third parties to record Zoom meetings without participants' knowledge, even if the host has removed participants' ability to record the meeting via the settings.[51] This problem does not appear to have been acknowledged or addressed by Zoom yet.

[47] Rae Hodge, *Zoom Security Issues: Zoom Buys Security Company, Aims for End-to-End Encryption*, CNET (May 8, 2020, 12:23 PM), https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/.
[48] *Id.*
[49] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (March 31 2020, 3:00 AM), https://theintercept.com/2020/03/31/zoom-meeting-encryption/.
[50] See Hodge, *supra*, note 45.
[51] *Id.*