

November 24, 2015

VIA ECFS

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554

**Stephanie A. Joyce**

Partner  
202.857.6081 DIRECT  
[stephanie.joyce@arentfox.com](mailto:stephanie.joyce@arentfox.com)

Re: WC Docket No. 12-375, Response to Letter from Martha Wright, et al.

Dear Secretary:

Securus Technologies, Inc. (“Securus”) hereby responds to the letter filed by the Martha Wright Petitioners on November 20, 2015 (“Wright Letter”).<sup>1</sup>

As the Commission is aware from Securus’s report, historical calling records were stolen from the custody of a third-party entity sometime in 2015. Securus has reported this theft in accordance with the Commission’s rules governing Customer Proprietary Network Information (“CPNI”). In addition, Securus immediately reported the theft to the FBI and U.S. Secret Service, and a computer forensics firm is investigating the circumstances of the theft. As Securus has stated to the Commission, there is no evidence that the incident was a “hack” by some third party. In addition, there is no evidence that conversations between inmates and their attorneys were recorded in error. Securus has issued two press releases which state these facts. **Attachments A and B.**

The Wright Letter, despite the author’s citation to Securus press releases, simply repeats the unfounded allegations of an online journalist. It then goes on to postulate a scenario in which other, completely unrelated types of information are stolen and then assigns liability to Securus for a hypothetical breach that has not occurred. The entire exercise is not only far-fetched and irresponsible, but dangerous and plainly was conceived to create panic. The Wright Letter is a disservice to the public interest.

The fallacy of the letter notwithstanding, Securus must assure the Commission and the public of the following:

---

<sup>1</sup> WC Docket No. 12-375, Letter from Lee G. Petro, Counsel to Martha Wright, et al., to Marlene H. Dortch, FCC (Nov. 20, 2015).

- The CPNI was stolen from a third-party entity to which Securus was required to provide CPNI but over which Securus had no control. Securus acquired that entity on October 31, 2015, and now has control over ensuring the security of all call-related information held by that entity.
- No financial information, credit card information, social security numbers, customer addresses, or any similar data was involved.
- The theft was limited to records from one correctional facility only, and was not a widespread theft.
- No theft, breach, leak, or hack of Securus's servers has occurred.
- No information obtained via Securus location-based services has been stolen.
- Securus is and has been aware of its obligations under the CPNI rules and is complying with them.

Please let me know if you need any further information from Securus. Thank you for your consideration.

Sincerely,

s/Stephanie A. Joyce

*Counsel to Securus Technologies, Inc.*

cc: Chairman Tom Wheeler  
Commissioner Mignon Clyburn  
Commissioner Jessica Rosenworcel  
Commissioner Ajit Pai  
Commissioner Michael O'Rielly  
Gig Sohn, Counselor to Chairman Wheeler  
Travis LeBlanc, Chief, Enforcement Bureau  
Rebekah Goodheart, Legal Advisor to Commissioner Clyburn  
Travis Litman, Legal Advisor to Commissioner Rosenworcel  
Nicholas Degani, Legal Advisor to Commissioner Pai  
Amy Bender, Legal Advisor to Commissioner O'Rielly  
Pamela Arluk, Chief, Pricing Policy Division, Wireline Competition Bureau  
Lynne Engledow, Acting Deputy Chief, Pricing Policy Division, Wireline Competition Bureau

*(All via electronic mail)*

# **ATTACHMENT A**

# PRESS STATEMENT

## **Securus Statement Regarding Media Reports of Leaked Call Records**

Securus is contacting law enforcement agencies in the investigation into media reports that inmate call records were leaked online. Although this investigation is ongoing, we have seen no evidence that records were shared as a result of a technology breach or hack into our systems. Instead, at this preliminary stage, evidence suggests that an individual or individuals with authorized access to a limited set of records may have used that access to inappropriately share those records.

We will fully support law enforcement in prosecution of any individuals found to have illegally shared information in this case. Data security is critically important to the law enforcement and criminal justice organizations that we serve, and we implement extensive measures to help ensure that all data is protected from both digital and physical breaches.

It is very important to note that we have found absolutely no evidence of attorney-client calls that were recorded without the knowledge and consent of those parties. Our calling systems include multiple safeguards to prevent this from occurring. Attorneys are able to register their numbers to exempt them from the recording that is standard for other inmate calls. Those attorneys who did not register their numbers would also hear a warning about recording prior to the beginning of each call, requiring active acceptance.

We are coordinating with law enforcement and we will provide updates as this investigation progresses.

# **ATTACHMENT B**

# PRESS STATEMENT

## Securus Provides Updates on Investigation into Stolen Data Records

November 13, 2015

### FOR IMMEDIATE RELEASE

DALLAS, TX November 13, 2015/PRNewswire/ -- Dallas, TX. – Securus Technologies continues to coordinate with law enforcement to investigate stolen data that was apparently provided to online outlet The Intercept according to the outlet’s report on November 11, 2015.

Securus takes this matter very seriously, and is working on multiple fronts to fully investigate the matter and to prevent future criminal attacks. In addition to reporting the situation to the FBI, Securus has retained a forensic data analysis firm to conduct a thorough review of all systems and procedures to verify how this particular incident occurred and to confirm it happened outside of the Securus network and systems. The forensics experts will also recommend any steps to further secure all customer and inmate information.

While still ongoing, Securus can provide several updates and clarifications on the status of its investigation:

- All information we have gathered to this point indicates that data provided to The Intercept were from a single customer’s data files and were likely accessed through a third-party vendor’s file-sharing arrangement, unique to that customer. We have not seen what was provided to The Intercept beyond what they’ve reported, but there is no indication at this point that the theft involved any other customer’s data nor that the data was obtained directly from the Securus network or platform.
- Despite allegations from The Intercept and other parties, we have seen no evidence to date of any attorney-client privileged communications that were recorded in error. While The Intercept reports that they matched call data from the stolen data with phone numbers attached to attorneys’ offices, no evidence has been provided that any of these calls were actually recorded, and if so, whether any of them would actually constitute privileged communications. Many calls from facilities are placed daily to law firms that are not subject to attorney client privilege including scheduling calls, informational queries, calls to people other than lawyers who work at law firms. There is a very important distinction between data that indicates that a call took place and an actual recording of the contents of that call. Data about the time and phone numbers of a

call are generated for virtually every call that is placed in the U.S., and it is not covered by attorney-client privilege.

Our calling systems include multiple safeguards to prevent attorney-client recordings from occurring. Licensed attorneys are able to register their numbers or a specific call to exempt them from recording. Attorneys and inmates who do not register their numbers or calls will hear a warning about recording prior to the beginning of each call, and both must actively acknowledge they want to continue the call.

While it is possible that not all of these safeguards were followed by the callers in some cases, we have seen no evidence to date of recorded calls that would fall under that category. Without direct access to the stolen information, Securus cannot confirm whether any such recorded calls exist. If such evidence exists, we encourage The Intercept or other parties with access to the stolen data to provide that information to the FBI.

- Contrary to some reports, Securus does not sell call recordings or information to our law enforcement or correctional customers or anyone else. We record calls and provide forensic software to our customers based on the stipulations of our service contracts and in accordance with federal, state and local laws. Retention of these records is also conducted according to laws in various jurisdictions.
- No credit card data, financial information, social security numbers or similar data from any party was contained in the information that was stolen. While this fact was never in question, we have received multiple questions on this front. Securus does not store credit card information.

Securus is fully committed to completion of a full investigation into this matter. We will use the results of the investigation to enhance the security of our operations wherever possible to help ensure that a similar situation does not occur in the future. We will provide updates as new information becomes available.