October 16, 2017

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Ex Parte Presentation, *Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281

Dear Ms. Dortch,

On October 12, 2017, Christopher Oatway (Verizon), Christopher Koegel (T-Mobile), Jacquelyne Flemming (AT&T), Kevin Rupy (USTelecom), Glenn Richards (Pillsbury, on behalf of Voice on the Net Coalition (VON)) via phone, and the undersigned of CTIA (collectively, provider representatives) met with Kurt Schroeder, Nancy Stevenson, Lauren Wilson, and Nellie Foosaner of the Commission's Consumer and Governmental Affairs Bureau to discuss the above-referenced proceeding.

During the meeting, the provider representatives expressed support for the Commission's goal to facilitate speedy access to blocked Caller ID information needed to investigate instances of threatening calls. Participants discussed aspects of the proposed Report and Order circulated by Chairman Pai[1] as outlined below.

I. Sharing Caller ID information with security personnel should be "as directed by law enforcement."

Provider representatives expressed support for the proposal to require providers to disclose Calling Party Numbers (CPN) to law enforcement representatives to address public safety needs, but raised concerns over the inclusion of "security personnel." The proposed Report and Order defines security personnel as "those individuals directly responsible for maintaining safety of the threatened entity consistent with the nature of the threat,"[2] such as "employees whose duties include security at an institution," or "corporate and government agency security personnel and school or university security

[1] *In the Matter of Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Draft Report and Order (rel. Oct. 3, 2017).
[2] *Id.* at 8.

staff acting within the scope of their duties."[3] We discussed specific examples, such as the issue that arose in the NASA Waiver,[4] or in instances of campus security.

However, the provider representatives expressed concern that, as drafted, the Report and Order may require providers to assess which persons appropriately qualify as "security personnel," a determination best made by law enforcement. The provider representatives expressed concern that there may be many other individuals who claim to be security personnel that providers will not be in a position to validate. It is actual law enforcement that has the necessary tools to assess who qualifies as security personnel.

For these reasons, the provider representatives recommended that Caller ID information only be provided to law enforcement, who can then determine what "security personnel" may be appropriate recipients of the information. Alternatively, if the Commission perceives a need for carriers to provide information to security personnel, the rules should make clear that the information should be provided "**as directed by law enforcement**."[5] This would ensure that law enforcement appropriately makes the determination of which entities sufficiently qualify as security personnel, while enabling providers to provide information that may be useful for public safety purposes.

II. Requests for Caller ID information should be made by law enforcement.

We expressed support for efforts to incorporate recommendations to require law enforcement involvement in the request, but raised concern with the ambiguity of the phrase "in conjunction with law enforcement." The draft Report and Order requires that requests for blocked Caller ID information associated with a threatening call "be made by the recipient of the threatening call in conjunction with law enforcement or by law enforcement on behalf of the threatened party."[6] This language creates ambiguity as to what level of involvement law enforcement must take in making these requests. This ambiguity, coupled with the potential requirement to share with additional security personnel, is concerning.

---

[3] *Id.* at 8, n. 59.

[4] *Rules and Policies Regarding Calling Number Identification Service – Caller ID; Petition of National Aeronautics and Space Administration for Waiver of Federal Communications Commission Regulations at 47 CFR. § 64.1601(b)*, CC Docket No. 91-281, Order, 27 FCC Rcd 5704 (CGB 2012) (NASA Waiver).

[5] So subpart (f) of Section 64.1601 would read: "…the carrier will provide any CPN of the calling party to ~~security personnel, if any, for the called party and to~~ law enforcement, **and to security personnel for the called party as directed by law enforcement,** for the purpose of identifying the party responsible for the threatening call."

[6] *Id.* at 8.

We recommended **eliminating the phrase "in conjunction with" from subpart (f) of Section 64.1601**, or alternatively, clarifying what is meant by "in conjunction with" law enforcement.

III. Requirements for use of secure communications may preclude rapid transmission of data.

Finally, we shared our concerns with the condition that all "transmission of restricted CPN information to and from law enforcement agencies and security personnel must occur only through secure communications."[7] While we appreciate the Commission incorporating recommendations to include restrictions and protections on the use of this information, we expressed our concern that the requirement to use secure communications may be impractical under the circumstances and could preclude the rapid transmission of this information to law enforcement by phone, as is frequently done in these emergency situations. Provider representatives discussed the processes already in place to authenticate callers and secure the information.

Given that providers already have rigorous processes in place to ensure the secure transmission of this information to law enforcement, that are specifically tailored to each situation and communication method used, we propose changing subpart (g)(4) of Section 64.1601 to read: "**(4) carriers transmitting restricted CPN information must take reasonable measures to ensure the security of such communications.**" This revision will ensure the security of the transmissions, without unnecessarily delaying transmission or disturbing existing processes that are highly effective.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed in ECFS and provided to the Commission participants. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Melanie K. Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy
CTIA

Matthew Gerst
Assistant Vice President, Regulatory Affairs
CTIA

[7] *Id.* at 9.

Kevin Rupy
Vice President, Law and Policy
USTelecom

Glenn S. Richards
Partner
Pillsbury

Cc: Kurt Schroeder
Nancy Stevenson
Lauren Wilson
Nellie Foosaner