Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Policies Regarding Calling Number Identification Service – Caller ID	)	CC Docket No. 91-281
	)	
	)	
Waiver of Federal Communications Commission Regulations at 47 C.F.R. § 64.1601(b) on Behalf of Jewish Community Centers	)	

REPLY COMMENTS OF NCTA – THE INTERNET & TELEVISION ASSOCIATION

NCTA – The Internet & Television Association (NCTA) submits these reply comments in response to the Commission's caller ID notice of proposed rulemaking, which proposes to make it easier to identify the origin of threatening calls.[1] NCTA supports amendment of the Commission's rules to allow providers to give blocked caller ID information related to threatening calls of a serious and imminent nature to law enforcement personnel upon request.

INTRODUCTION

Under the current rules, a party that receives a threatening call from a blocked number must seek a waiver from the Commission before a provider may release Calling Party Number (CPN) information associated with the call.[2] In the *NPRM* the Commission recognizes that such case-by-case waiver determinations can "hinder[] a rapid response to the threat."[3] To eliminate this unnecessary delay, NCTA supports the Commission's proposal for a more streamlined

---

1 *Rules and Policies Regarding Calling Number Identification Service – Caller ID; Waiver of Federal Communications Commission Regulations at 47 C.F.R. § 64.1601(b) on Behalf of Jewish Community Centers*, CC Docket No. 91-281, Notice of Proposed Rulemaking, 32 FCC Rcd 8342 (June 22, 2017) (*NPRM*).

2 47 C.F.R. §64.1601(b) (prohibiting carriers from overriding a calling party's request to block CPN).

3 *NPRM*, 32 FCC Rcd at 5342, ¶2.

approach that would enable service providers to disclose blocked CPN information in connection with threatening calls.

In considering its proposed approach, the Commission appropriately recognizes that it must ensure that the CPN rules are "not abused and that the legitimate privacy interests of non-threatening callers are not infringed."[4] Toward that end, NCTA agrees with other commenters that: (1) a law enforcement agency should determine whether a call is threatening; and (2) a service provider should disclose CPN information only to the law enforcement agency that makes this determination.

I. A LAW ENFORCEMENT AGENCY SHOULD DETERMINE WHAT CONSTITUTES A THREATENING CALL

The Commission should adopt its proposal to require that blocked CPNs be made available only after a law enforcement agency confirms that a call constitutes a serious and imminent threat.[5] Law enforcement agencies have the authority and expertise to most efficiently, accurately, and consistently make such determinations. These agencies certainly are in a better position to do so than a service provider's customer support or call center personnel.

As AT&T points out, law enforcement personnel are in a much better position than are provider employees "to avoid being misled by those who inevitably would seek to exploit this potential opportunity to obtain restricted Caller ID information of non-threatening callers through misrepresentation in order to stalk a separated spouse or engage in other illicit activity."[6] CTIA also notes, "It is not hard to imagine circumstances in which a party falsely reports a threatening call in order to unmask legitimately blocked CPN . . . Requiring law enforcement to

---

4 *Id.* at 5347, ¶15.

5 *Id.* at 5347, ¶13.

6 AT&T Comments, CC Docket No. 91-281, at 6 (Aug. 21, 2017) (AT&T Comments).

make the determination and receive information will deter parties from manipulating the unblocking process."[7]

In addition, the Commission should adopt commenters' proposal to match the definition of a "threatening call" under the caller ID rules with the disclosure requirements under the Electronic Communications Privacy Act (ECPA).[8] Specifically, the Commission should define a threatening call under section 64.1600 as "any call that includes a threat involving danger of death or serious physical injury to any person."

II. SERVICE PROVIDERS SHOULD DISCLOSE BLOCKED CPN ONLY TO A LAW ENFORCEMENT AGENCY UNDER THE RULES

NCTA agrees with initial commenters that any exception to the caller ID disclosure rules should allow service providers to disclose CPN only to the law enforcement agency that confirms the existence of a threatening call.[9] That law enforcement agency then should have the discretion to provide the CPN information to any other parties that have a lawful claim to the information. The rule exception should not authorize blocked CPNs to be disbursed to non-law enforcement entities; such entities may continue to use the Commission's waiver process to obtain access to blocked CPNs.

Limiting service providers' CPN disclosure obligations only to law enforcement agencies under the caller ID rules represents the best way to balance both privacy and public safety concerns in the context of the broader CPN exemption that the Commission now proposes to implement.

---

7 CTIA Comments, CC Docket No. 91-281, at 8 (Aug. 21, 2017) (CTIA Comments).

8 AT&T Comments at 3-4; CTIA Comments at 6-7; 18 U.S.C. § 2702(c)(4).

9 AT&T Comments at 6; CTIA Comments at 8.

When prior case-by-case waivers have been granted to non-law enforcement entities, these narrow approvals have been conditioned "on implementation of several safeguards consistent with the privacy objectives of the CPN rules to protect the confidentiality of calling parties."[10] For example, the Commission limited CPN access to "telecommunications and security personnel" and "only when investigating phone calls of a threatening and serious nature."[11] The Commission also required that such access be documented as part of an investigative report and that any violation of these conditions "be reported promptly to the Commission."[12] In adopting these conditions, the Commission concluded that the "likelihood that CPN information will be disclosed to unauthorized personnel is minimized and, hence, any legitimate expectation of privacy by the caller is adequately addressed."[13]

These case-by-case waiver decisions permitted limited access to CPN information by non-law enforcement personnel during an investigation. There is no practical way, however, for the Commission to enforce similar limitations if it adopts a generally applicable exemption from the CPN non-disclosure requirements for threatening calls. For example, unless it constrains disclosure to law enforcement agencies, CPN could be disclosed to individuals, small businesses, or others that simply do not have "telecommunications and security personnel." Given that the

---

[10] *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 C.F.R. § 64.1601(b)*, CC Docket No. 91-281, Order, 27 FCC Rcd 5704, 5708, ¶12 (CGAB 2012).

[11] *Rules and Policies Regarding Calling Number Identification Service – Caller ID, Waiver of the Federal Communications Commission Regulations at 47 C.F.R. § 64.1601(b) on Behalf of Jewish Community Centers*, CC Docket No. 91-281, Temporary Waiver Order, 32 FCC Rcd 1559, 1564, ¶10 (CGAB 2017) (*JCC Order*); *Rules and Policies Regarding Calling Number Identification Service – Caller ID, Petition of Enlarged City School District of Middletown for Waiver of Federal Communications Commission Regulations at 47 C.F.R. § 64.1601(b)*, CC Docket No. 91-281, Order, 31 FCC Rcd 3565, 3569, ¶13 (CGAB 2016); *Rules and Policies Regarding Calling Number Identification Service – Caller ID, Petition of Liberty Public School District for Waiver of Federal Communications Commission Regulations at 47 C.F.R. § 64.1601(b)*, CC Docket No. 91-281, Order, 28 FCC Rcd 6412, 6417, ¶13 (CGAB 2013).

[12] *Id*.

[13] *JCC Order*, 32 FCC Rcd at 1563, ¶11.

Commission would not even know which parties were provided with blocked CPN information, it also would be impossible for the Commission to ensure that: (1) CPN information is not used for unauthorized purposes, (2) such information is not disclosed to unauthorized parties, or (3) any unauthorized disclosures are reported to the Commission. Instead, the law enforcement agency with insight into the specific threatening call at issue would be better positioned to appropriately limit disclosure of blocked CPN information.

Put simply, limiting access to law enforcement would appropriately protect privacy concerns by ensuring that access to blocked CPN information is not released too broadly while simultaneously fulfilling the public safety need to provide those actively investigating a threatening call with timely access to CPN information.

CONCLUSION

As discussed above, NCTA supports the Commission's proposal to adopt an exception to its caller ID rules to allow disclosure of blocked CPN related to threatening calls, and urges the Commission to ensure that a "threatening call" is defined consistent with ECPA; that law enforcement authorities determine whether a call meets this definition; and that blocked CPNs under this exception are made available only to law enforcement personnel.

Respectfully submitted,

/s/ Steven F. Morris

Steven F. Morris
Jennifer K. McKee
NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431

September 19, 2017