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	)	
	)	

COMMENTS OF CTIA

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

August 21, 2017

Table of Contents

I. INTRODUCTION AND SUMMARY 1

II. THE FCC HAS USED COMMON SENSE WHEN ITS CALLER ID RULES HAVE BECOME OBSTACLES TO PUBLIC SAFETY. 2

III. FCC CALLER ID RULES SHOULD NOT BE AN IMPEDIMENT TO LAW ENFORCEMENT INVESTIGATIONS AND EMERGENCY RESPONSES. 5

A. The FCC's Proposal Risks Creating Unnecessary Tensions and Complexities. 6

B. The FCC's Proposal Should Be Narrowed. 10

IV. THE FCC SHOULD CONTINUE EXISTING WAIVERS AND CONSIDER STREAMLINING REVIEW WHERE PRIVATE PARTIES NEED UNBLOCKED CALLER ID. 11

V. CONCLUSION 12

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	)	
	)	

COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY

CTIA[1] submits these comments in response to the Notice of Proposed Rulemaking ("*NPRM*") by the Federal Communications Commission ("FCC" or "Commission") proposing a rule change to address the troubling practice of callers using a blocked phone number to make threatening calls, including calls to schools, religious organizations, and other entities.[2]

CTIA applauds the Commission's past waiver grants, particularly in response to the recent threatening calls against religious organizations and communities. To achieve the Commission's goal of ensuring that "law enforcement personnel have quick access to the

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st- century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *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*, Notice of Proposed Rulemaking, FCC 17-76, CC Docket No. 91-281 (June 22, 2017) ("*NPRM*").

information they need to identify and thwart threatening callers,"[3] CTIA supports a revision to 47 C.F.R. § 64.1601, to ensure that carriers' existing obligation to respect a calling party's request to block caller ID is not an impediment to law enforcement. Specifically:

- The FCC should adopt a fourth exception to 47 C.F.R. § 64.1601(d) that makes clear that Section 64.1601(b) is not an obstacle to providing unblocked Calling Party Numbers ("CPN") information in response to valid law enforcement requests for assistance.
- The FCC should not impose a new mandate on carriers to provide unblocked calling party information, and it should not require or authorize the sharing of that information with third parties other than law enforcement.
- The FCC should preserve existing waivers, and continue to use its waiver process where third parties meet the good cause standard to receive blocked caller ID information, and consider ways to streamline that process. The current waiver process has given repeatedly threatened parties a way to ensure appropriate personnel have access to the information needed to identify and thwart threatening callers and waivers should continue to be issued to qualifying entities.

This proceeding is one component of industry and FCC work to improve how calls are identified and authenticated. The Commission should evaluate caller ID policy in the context of ongoing industry and shared efforts to abate illegal robocalling and improve call authentication.

II. THE FCC HAS USED COMMON SENSE WHEN ITS CALLER ID RULES HAVE BECOME OBSTACLES TO PUBLIC SAFETY.

The Commission's caller ID rules generally prohibit carriers from transmitting calling party number ("CPN") when the caller has so requested by dialing *67.[4] A terminating carrier must act in accordance with the caller's privacy indicator, subject to three exceptions: when calling party CPN delivery (i) is used within limited systems; (ii) is used in connection with 911 or poison control lines; or (iii) is provided in connection with "legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency."[5] The Commission's

---

3 *NPRM* ¶ 3.

4 47 C.F.R. §§ 64.1601(a), (b).

5 *Id.* § 64.1601(d)(4)(i)-(iii).

objective in adopting Section 64.1601 was "to establish federal policies governing the passage by carriers of CPN on interstate calls," and to protect privacy interests of callers, by requiring carriers to "provide callers the option of withholding their numbers from called parties on a per call basis."[6]

In some instances, the blocking of caller ID has complicated the delivery of essential services, so the Consumer and Governmental Affairs Bureau has granted waivers of the CPN privacy option. The FCC has relied on a "good cause" standard,[7] granting limited waivers where a petitioner has demonstrated that the waiver will serve the public interest. For instance, the Commission has granted waivers to entities that provide emergency services but faced difficulties identifying callers and dispatching aid when callers had blocked caller ID.[8] The Commission has not lightly awarded waivers, and imposes rigorous conditions on recipients. For example, in some instances, waiver recipients are directed to take special precautions to ensure that access to CPNs will be used only for "investigating phone calls of a threatening and

---

6 *Rules and Policies Regarding Calling Number Identification Service – Caller ID*, Report and Order and FNPRM, 9 FCC Rcd 1764, ¶ 48 (1994) ("*Caller ID Order*").

7 The Commission may waive any of its rules "for good cause shown." 47 CFR § 1.3; *See WAIT Radio v. FCC*, 418 F.2d 1153 (D.C. Cir. 1969), *appeal after remand*, 459 F.2d 1203 (D.C. Cir. 1972), *cert. denied*, 409 U.S. 1027 (1972); *Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164 (D.C. Cir. 1990).

8 *See, e.g.*, *INSIGHT 100 Petition for Waiver of §64.1601(b) Regarding the Transmission of Calling Party Number*, Memorandum Opinion & Order, 17 FCC Rcd 223 (CCB 2002) (waiving Section 64.1601(b) on behalf of certain universities and hospitals); *Petition of Chevrah Hatzalah Volunteer Ambulance Corps Inc. for Waiver of Section 1601(b) of the Commission's Rules*, Order, 28 FCC Rcd 1253 (CGB 2013) ("Hatzalah Order").

serious nature."[9] Recently, the Bureau prudently waived the rule in response to school districts that received repeated, serious threats.[10]

This proceeding arises in part out of requests from schools, Jewish Community Centers ("JCCs"), and other religious organizations for waivers of the CPN privacy obligation, in order to respond to phone calls threatening acts of violence.[11] The waivers were granted to help ensure that JCCs and law enforcement would not be hindered by Section 64.1601(b) in obtaining CPN to identify callers using blocked numbers to make threats.

CTIA shares the FCC's interest in addressing threatening calls. While unblocking CPN information can help identify threatening callers in some circumstances, it may not by itself solve investigations.[12] Recent threats to JCCs and others were often not perpetrated simply by blocking caller ID.[13] As with the JCC's calls, many illegal calls are spoofed and routed

---

9 *See, e.g.*, *Petition of Enlarged City School District of Middletown for Waiver of Federal Communications Commission Regulations at 47 CFR 64.1601(b)*, Order, 31 FCC Rcd 3565, ¶ 13 (CGB 2016) ("Middletown Waiver").

10 *Petition of Liberty Public School District for Waiver of Federal Communications Commission Regulations at 47 CFR § 64.1601(b)*, Memorandum Opinion and Order, 28 FCC Rcd 6412 (CGB 2013); Middletown Waiver.

11 *Waiver of Federal Communications Commission Regulations at 47 CFR 64.1601(b) on Behalf of Jewish Community Centers*, Temporary Waiver Order (DA 17-223) (Mar. 3, 2017) ("JCC Temporary Waiver Order").

12 For example, in April 2017, the United States charged an individual with making hundreds of threatening calls to JCCs. *See United States v. Kadar*, 17-mj-1361 (M.D.Fl. 2017) (available at: https://www.justice.gov/opa/press-release/file/959491/download). The Complaint detailed the steps the individual took to mask his identity, including using a "Spoofing Company" that allowed him to disguise his voice as female and eliminate his speech impediment. *Id.* at ¶¶ 7-9, 20, 26. The caller used multiple VOIP accounts, which he accessed through proxies and virtual private networks to hide his true IP address. *Id.* The caller further used a "large parabolic antenna" which allowed him to access open Wi-Fi networks from significant distances. *Id.* Merely unblocking his CPN would not have been sufficient to defeat these anonymizing measures.

13 *Id.*

internationally, meaning that unmasking the CPN will not necessarily help identify the culprit. The wireless industry has and will continue to work collaboratively with public and private stakeholders on call authentication methods which will help consumers and carriers limit the misuse of telephone networks.

III. FCC CALLER ID RULES SHOULD NOT BE AN IMPEDIMENT TO LAW ENFORCEMENT INVESTIGATIONS AND EMERGENCY RESPONSES.

The Commission proposes to amend the Caller ID rules to enable both called parties and law enforcement to obtain blocked Caller ID information in instances of threatening calls. CTIA supports amending the caller ID rules to enable rapid assistance to law enforcement and the victims of crimes. However, the Commission's proposal raises concerns and may result in unintended complexity, so CTIA suggests the Commission narrow its approach.

Currently, carriers operate under several laws and regulations that restrict their handling of customer information. Section 64.1601(b) of the Commission's rules requires that a carrier act in accordance with the customer's request that CPN not be passed on interstate calls. Section 64.1601(d) creates a few exceptions to this rule, such as when CPN delivery "[i]s provided in connection with legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency."[14] A different set of requirements comes from the Electronic Communications Privacy Act (ECPA), which governs when a carrier can or must disclose customer communications or records.[15] For example, 18 U.S.C. § 2702(a) restricts the disclosure of customer information, but Section 2702(c) states that a provider *may* divulge a record or other information pertaining to a subscriber or customer "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to

---

14 47 C.F.R. § 64.1601(d)(4)(ii).

15 *See* 18 U.S.C. §§ 2701, et seq.

any person requires disclosure without delay of information relating to the emergency."[16] *Mandatory* disclosures are described in 18 U.S.C. § 2703. For example, Section 2703(c)(2)(E) states that a provider must provide a "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address" in response to particular types of process.[17] These obligations create a predictable regime with clear rights and obligations, as well as protections for privacy.

A. The FCC's Proposal Risks Creating Unnecessary Tensions and Complexities.

The FCC proposal would impose an unnecessary new mandate on carriers that creates tension with federal law. The FCC proposes to create an affirmative obligation on carriers to act. Such an obligation is inconsistent with the structure of both the ECPA and the FCC's regulations described above. The current regulatory scheme enables CTIA's members to assist law enforcement in investigations and emergencies by allowing carriers to disclose information on a voluntary basis when certain exceptions are met. The *NPRM*'s proposed disclosure mandate creates tension with this regime. Any new exceptions should work in harmony with the existing exceptions, and be stated as a true exception, rather than take the form of a new duty. The wireless industry's long and successful track record of cooperation with law enforcement requests, even in the absence of an affirmative obligation, demonstrates that a new mandate is not necessary.

The proposed rule states that "[u]pon report of such a threatening call, the carrier *will provide* any CPN of the calling party to the called party and/or law enforcement for the purpose

---

16 18 U.S.C. § 2702(c)(4). 18 U.S.C. § 2702(b)(8) has a similar provision for disclosure of communications content under similar circumstances.

17 18 U.S.C. § 2703(c)(2)(E).

of identifying the responsible party."[18] This requires carriers to act when someone reports to the carrier "any call that includes a threat of serious and imminent unlawful action posing a substantial risk to *property, life, safety, or health.*"[19] Existing federal law prohibits a provider of "electronic communication service to the public" from "knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of such service."[20] It contains an exception that *permit*s disclosure—but does not *require* it—in some emergencies. Specifically, carriers may disclose customer information to the government "if the provider, in good faith, believes that an emergency involving danger of *death or serious physical injury to any person* requires disclosure without delay of information relating to the emergency."[21]

The FCC's proposed mandate is broader than the current emergency exception under federal law. The exception under Section 2702 is limited to emergencies involving "death or serious physical injury to any person,"[22] but does not include emergencies that involve, for example, risks to property. If adopted, the FCC's mandate would require carriers to disclose CPN information in situations involving risks related to property (such as a call threatening to steal a car). The FCC's mandate would *require* disclosure of caller information that existing federal law does not permit. The proposed regime risks creating uncertainty by putting carriers in the difficult position of being required to do something by FCC rule that is not authorized by Section 2702 or protected by Section 2703.

---

18 *NPRM*, APPENDIX A.

19 *NPRM* ¶ 12 (emphasis added).

20 18 U.S.C. § 2702(a).

21 *Id.* § 2702(c)(4) (emphasis added).

22 *Id.*

The draft rule contemplates providing information directly to called parties and would potentially require carriers to make judgments about what constitutes a "threatening call." As an initial matter, it is unclear whether the FCC is proposing that a carrier would be required to turn over CPN to any caller who reaches out purporting to have received a "threatening call," or whether the carrier will be responsible for determining whether a threatening call occurred, but either proposition is problematic.

A regime to provide information in response to a report of a "threatening call," will create complexity and invite unintended consequences. The plain language of the proposal suggests a carrier would be required to hand over CPN to any caller alleging to have received a threatening call. This risks opening the door to abuse by third parties, as the FCC suspected would be possible.[23] It is not hard to imagine circumstances in which a party falsely reports a threatening call in order to unmask legitimately blocked CPN, and the proposed rule as drafted, may not permit a carrier to decline. Requiring law enforcement to make the determination and receive information will deter parties from manipulating the unblocking process.

Alternatively, the proposed rule suggests that responsibility for determining whether a "threatening call" has been made will fall to carriers, instead of law enforcement, which is best equipped to evaluate criminal activities including threats of violence or other illegal activity. Requiring carriers to evaluate threats would increase risks of error or confusion. Carriers do not routinely engage in the subjective evaluation of threats, and they are in no position to judge whether a reported call involves a threat of "unlawful action" or what is a "substantial risk" of

---

[23] *NPRM* at ¶ 15 (asking "whether we should require anyone reporting a threatening call for purposes of obtaining otherwise restricted CPN to do so in conjunction with a law enforcement agency, so as to provide some assurance that the called party is not attempting to circumvent the privacy obligations of the rule by reporting a false threat.")

harm. Generally, carriers rely on assertions by law enforcement of emergencies that provide a good faith belief in a "danger of death or serious physical injury" that meets the standard in Section 2702(c)(4). This is sensible, because law enforcement personnel have the training and experience to evaluate calls purported to be threatening or illegal. In many cases, they may be familiar with the called party and situation, improving the reliability of requests. *Finally*, even if it were reasonable to expect a carrier to make judgment calls about the veracity of a report or the severity or urgency of a claimed threat, carriers may need to employ trained staff around-the-clock to respond to "threatening calls." This complex task would be on top of existing subpoena compliance teams that process government assistance and emergency requests. And, having carriers evaluate threats may subject them to potential liability for incorrect judgment calls.[24] Law enforcement has the experience and the thousands of officers in communities throughout the country who are already positioned to evaluate whether a threat is genuine. It is unrealistic to expect carriers to replicate law enforcement's capability to do so.

The draft rule would require unrestricted disclosure directly to called parties, which raises concern. The proposed new rule contemplates providing unblocked CPN directly to called parties with no restrictions on its use. This invites the sort of manipulation described above. Providing information to the called party is inconsistent with conditions imposed by the FCC in past waivers dealing with instances like those contemplated here.[25] For example, the Commission required in the JCC Order that "the CPN on incoming restricted calls to JCCs *may not be passed on to the line called*," and limited JCC access to approved personnel, among other

---

[24] Indeed, if the Commission adopts a regime where carriers are responsible for evaluating the nature of threatening calls, the Commission should include a safe harbor provision to insulate the carrier from liability. A carrier should not incur legal exposure for providing CPN in response to what the carrier in good faith believes to be a lawful request.

[25] *NPRM* n.41.

restrictions that, in its view, protected the calling party's interests.[26] In other waivers, the petitioner "commit[ted] to accessing the information only for [a] limited purpose" and to abide by restrictions on its use and handling.[27] The Commission asks whether similar conditions should be imposed on any parties who receive protected CPN under a new regime.[28] Called parties should not be the recipients of information. But if the FCC determines some should receive it, use of disclosed CPN should be restricted—by rule—in a manner consistent with conditions in prior waivers.

B. The FCC's Proposal Should Be Narrowed.

The FCC should tailor its approach to avoid the complexities that attend its proposed rule. The Commission can avoid tension with federal law and reaffirm a provider's ability to provide blocked CPN by clarifying its rule. There are several ways the FCC could adjust its proposal. One possibility is to add an exemption in Section 64.1601(d), that would harmonize the rule with federal law, including Section 2702(c)(4). The provision would state that Section 64.1601(b)'s prohibition overriding a privacy indicator does not apply when "CPN delivery… (iv) Is provided in connection with any lawful request by a law enforcement agency for assistance in an emergency." This would preserve the permissive nature of emergency assistance under Section 2702 and the protections of Section 2703 while ensuring that Section 64.1601(b) is not an obstacle. Such an approach would obviate the need for the FCC to define a new category of "threatening call" and prevent carriers from having to make difficult judgment calls in

---

26 JCC Order ¶ 10 (emphasis added).

27 *See, e.g.* Middletown Order at ¶¶ 10, 13.

28 *NPRM* at ¶ 16.

sensitive situations. This would also remove any doubt that providers can respond to bona fide law enforcement requests that involve CPN.

IV. THE FCC SHOULD CONTINUE EXISTING WAIVERS AND CONSIDER STREAMLINING REVIEW WHERE PRIVATE PARTIES NEED UNBLOCKED CALLER ID.

CTIA supports the Commission continuing the existing waivers and issuing additional waivers as needed, perhaps under streamlined processes or rules tailored to types of organizations. Issuance of waivers is undoubtedly appropriate where law enforcement and threatened parties' security and telecommunications personnel need access to caller information on an ongoing basis and without delay.

Private parties being threatened can seek waivers, perhaps under a streamlined process. There may be situations where, with proper privacy and data protections, permitting a called party to have broad access to unblocked CPN is merited. However, the relative rarity of such situations—only six waivers have been issued in the last 15 years—indicates that a permanent policy of disclosure to called parties is unnecessary. To protect parties with legitimate needs to identify blocked callers, the FCC might consider procedural changes to expedite waiver requests, including allowing law enforcement agencies to request or support expedited treatment for apparent victims. At present, consideration of waiver requests can take as little as two months or more than a year.[29] Given the interests at stake, the FCC may consider how to more expeditiously consider such requests.

If restricting the exemption to law enforcement excludes public safety or other entities that the FCC thinks should be covered, the FCC can amend its rules to cover appropriate types

[29] *See* Middletown Waiver (filed Feb. 18, 2016, granted Apr. 13, 2016); Hatzalah Order (filed Sept. 30, 2011; granted Feb. 20, 2013).

of organizations. The current rule exempts 911 and poison control centers. Private ambulance and security companies may benefit from being exempt, but do not satisfy the current exemption. If the FCC believes that certain types of entities, like those who received past waivers, need prospective relief from the caller ID rules, it can tailor its rules to them instead of creating a broad new mandate. For example, the second exemption in Section 64.1601(d) for CPN delivery "used on a public agency's emergency telephone line or in conjunction with 911 emergency services, or on any entity's emergency assistance poison control telephone line" could be amended to add "or another approved private entity's" before "emergency telephone line." The Commission could separately consider or enumerate what sort of private entities might be appropriately included in a broadened exemption.

V. CONCLUSION

CTIA's members stand ready to assist law enforcement with investigations of threatening calls using blocked caller ID information. The proposals outlined in these comments balance the need to enable law enforcement's rapid response with communications providers' resources and obligations under existing law.

Respectfully submitted,

By: *s/ Melanie K. Tiano*

Melanie K. Tiano
Director, Cybersecurity and Privacy
Thomas C. Power
Senior Vice President, General Counsel
Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

August 21, 2017