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	)	

REPORT AND ORDER

Adopted: October 24, 2017 **Released: October 25, 2017**

By the Commission: Chairman Pai and Commissioners Clyburn, O'Rielly and Carr issuing separate statements.

I. INTRODUCTION

1. Today, we help security and law enforcement personnel obtain quick access to blocked Caller ID information needed to identify and thwart threatening callers. We also amend our rules to allow non-public emergency services to obtain blocked Caller ID information associated with calls requesting assistance.

2. The number of threatening phone calls has increased dramatically in recent years.[1] These calls traumatize communities and result in substantial disruption to schools, religious organizations, and other entities. They also drain public resources by requiring the deployment of police and bomb units. Schools and others receiving threats have suggested that blocked Caller ID information hinders a rapid response.[2] Our action today moves away from case-by-case waivers[3] to a streamlined approach that will help protect the safety of threatened parties in a timely way.

---

[1] *See, e.g.*, Eric Levenson and AnneClaire Stapleton, Jewish Center Bomb Threats Top 100; Kids Pulled from Schools (Mar. 13, 2017), http://www.cnn.com/2017/02/28/us/bomb-threats-jewish-centers-jcc/ (reporting over 100 threats to 80 Jewish Community Centers); Associated Press, Statistics: Bomb Threats to Schools in New Hampshire are Up (Aug. 21, 2016), http://www.washingtontimes.com/news/2016/aug/21/statistics-bomb-threats-to-schools-in-new-hampshir/ (reporting an increase in threats to New Hampshire schools); United States Bomb Data Center, Bomb Threats across the U.S. (May 24, 2016), https://www.atf.gov/resource-center/docs/bomb-threats-across-us/download (finding an 84% increase in bomb threats to schools from 2010-2016 and an increase in bomb threats to residences) (ATF Report); Richard J. Bayne, Swatting Epidemic 'out of control' in Middletown School District (Feb. 27, 2016), http://www.recordonline.com/news/20160227/swatting-epidemic-out-of-control-in-middletown-school-district (reporting a rash of threats made to various schools in New York and the adverse impact on students); James Fisher, More School Threats in Region; FBI Assisting (Jan. 19, 2016), http://www.delawareonline.com/story/news/local/2016/01/19/fresh-round-school-threats-tuesday/78999668/ (reporting multiple phone threats to schools in Delaware, Virginia, Maryland, and Massachusetts).

[2] *See*, *e.g.*, *Petition of Enlarged City School District of Middletown for Waiver of Federal Communications Commission Regulations at 47 C.F.R. 64.1601(b)* at 5 (filed Feb. 29, 2016) (*Middletown Petition*) (confirming that it has been hindered by section 64.1601(b) in identifying threatening callers).

II. BACKGROUND

A. The CPN Rules

3. In 1994, the Commission adopted rules that require common carriers using Signaling System 7 (SS7) to transmit the Calling Party Number (CPN)[4] on interstate calls to interconnecting carriers.[5] The Commission concluded that passage of CPN over interstate facilities made possible a wide range of services, and that promoting the development of such services was consistent with the Commission's responsibilities under the Communications Act of 1934, as amended (the Act).[6] In particular, the Commission concluded that requiring CPN transmission would bring consumers more rapid and efficient service, and encourage the introduction of new technologies and services to the public.[7]

4. In adopting this requirement, however, the Commission recognized that unrestricted CPN transmission could intrude upon the privacy interests of calling parties wishing to remain anonymous.[8] Therefore, the Commission established privacy options to allow callers to restrict the transmission of their telephone numbers.[9] For example, the Commission's rules require carriers using SS7 to recognize the dialing of *67 as a request that the carrier not pass the calling party's number.[10] Section 64.1601(b) of the Commission's rules provides that "[n]o common carrier subscribing to or offering any service that delivers CPN may override the privacy indicator associated with an interstate call."[11]

5. The former Common Carrier Bureau and the Consumer and Governmental Affairs Bureau (CGB or the Bureau) have granted limited waivers of the CPN privacy options in specific

(Continued from previous page)

[3] *See*, *e.g.*, *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 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 CFR 64.1601(b)*, CC Docket No. 91-281, Order, 31 FCC Rcd 3565 (CGB 2016) (*Middletown Order*).

[4] The Commission's rules define CPN as "the subscriber line number or the directory number contained in the calling party number parameter of the call set-up message associated with an interstate call on a Signaling System 7 network." 47 CFR § 64.1600(e). Associated with the CPN is a Privacy Indicator "that indicates whether the calling party authorizes presentation of the calling party number to the called party." 47 CFR § 64.1600(j).

[5] *See Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 1764 (1994) (*Caller ID Order*); *see also* 47 CFR § 64.1601(a).

[6] *Caller ID Order*, 9 FCC Rcd at 1769, para. 34.

[7] *Id.* at 1766, para. 8.

[8] *Id.* at 1769, para. 34.

[9] *See* 47 CFR § 64.1601(b); *see also Rules and Policies Regarding Calling Number Identification Service – Caller ID*, Memorandum Opinion and Order on Reconsideration, Second Report and Order and Third Notice of Proposed Rulemaking, CC Docket No. 91-281, 10 FCC Rcd 11700, 11728-29, paras. 81-84 (1995) (*Caller ID Reconsideration Order*).

[10] 47 CFR § 64.1601(b). In addition, carriers providing privacy on all calls dialed from a particular line will recognize dialing *82 as a caller's request that the CPN be passed through on an interstate call. *See Caller ID Reconsideration Order*, 10 FCC Rcd at 11728-29, paras. 81-84; *see also* 47 CFR § 64.1601(b).

[11] Section 64.1601(b) also provides that, "[c]arriers must arrange their CPN-based services, and billing practices, in such a manner that when a caller requests that the CPN not be passed, a carrier may not reveal that caller's number or name, nor may the carrier use the number or name to allow the called party to contact the calling party." 47 CFR § 64.1601(b).

instances where requesting parties have demonstrated that such waivers serve the public interest.[12] For example, the Bureau has waived the rule in response to requests from school districts that had received bomb threats, while at the same time ensuring that access to CPNs would be very limited.[13] In addition, the Commission has found that in certain limited circumstances, the privacy requirements for CPN-based services should not apply to delivery of the CPN to a public agency's emergency line, a poison control line, or in conjunction with 911 emergency services.[14]

B. The Notice of Proposed Rulemaking

6. In the June 2017 *Caller ID NPRM*, the Commission proposed to amend its rules to ensure that security and law enforcement personnel have quick access to the Caller ID information they need to identify and thwart threatening callers, without the regulatory delay inherent in applying for and being granted a waiver of the rules.[15] The *Caller ID NPRM* proposed an exemption from privacy protections that would allow the provision of blocked Caller ID information in the limited case of threatening calls.[16] It also sought comment on how to define a "threatening call"[17] and on whether to require anyone seeking blocked Caller ID information to do so in conjunction with a law enforcement agency to ensure that the called party is not attempting to circumvent the privacy obligations of the rule by reporting a false threat.[18] Finally, the Commission asked whether to extend an existing exemption for public emergency services to non-public entities that provide emergency services, such as private ambulance companies, so that they can readily obtain blocked Caller ID information for callers who request assistance.[19] Eight entities and individuals filed comments and three entities filed reply comments in response to the *Caller ID NPRM*, and all support addressing the problem of threatening calls with blocked Caller ID, albeit with varying recommendations on how to do so.[20]

---

[12] *See INSIGHT 100 Petition for Waiver of § 64.1601(b) Regarding the Transmission of Calling Party Number*, CC Docket No. 91-281, Memorandum Opinion and Order, 17 FCC Rcd 223 (CCB 2002) (*INSIGHT Order*) (waiving section 64.1601(b) on behalf of certain universities and hospitals); *Rules and Policies Regarding Calling Number Identification Service – Caller ID; Petition of Chevrah Hatzalah Volunteer Ambulance Corps Inc. for Waiver of Section 1601(b) of the Commission's Rules – Blocked Telephone Numbers*, CC Docket No. 91-281, Order, 28 FCC Rcd 1253 (CGB 2013) (*Hatzalah Order*); *Petition of Liberty Public School District for Waiver of Federal Communications Commission Regulations at 47 CFR § 64.1601(b)*, CC Docket No. 91-281, Memorandum Opinion and Order, 28 FCC Rcd 6412 (CGB 2013) (*Liberty School Order*); *Middletown Order,* 31 FCC Rcd at 3565.

[13] *See, e.g.*, *id.*, 31 FCC Rcd at 3567-58, paras. 5-8; *Liberty School Order*, 28 FCC Rcd at 6414-15, paras. 5-6.

[14] *Caller ID Order*, 9 FCC Rcd at 1770, para. 37; *see also* 47 CFR § 64.1601(d)(4)(ii). Our rules also exempt "legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency." 47 CFR § 64.1601(d)(4)(iii).

[15] *Rules and Policies Regarding Calling Number Identification Service — Caller ID*, CC Docket No. 91-281, Notice of Proposed Rulemaking, 2017 WL 2714970 (2017) (*Caller ID NPRM*).

[16] *Id.* at para. 1.

[17] *Id.* at para. 12.

[18] *Id*. at para. 13.

[19] *Id*. at para. 14.

[20] *See*, *e.g.*, AT&T Services Aug. 21, 2017 Comments at 1 (AT&T Comments) ("AT&T strongly supports the adoption of an additional exception the Caller ID privacy rules . . . the Commission should structure this exception to be consistent with the requirement for carriers' . . . established by the Electronic Communications Privacy Act (ECPA)."); Chevrah Hatzalah Volunteer Ambulance Corps Inc. Aug. 21, 2017 Comments at 3 (Hatzalah Comments) ("Hatzalah strongly supports the Commission's efforts to help combat the rise in threatening phone calls."); CTIA Aug. 21, 2017 Comments at 1 (supporting quick access to blocked Caller ID, but expressing a preference for the Commission continuing to use the waiver process). In addition, AT&T suggests that the Commission undertake further efforts to thwart Caller ID "spoofing." AT&T Aug. 21, 2017 Comments at 6. "Spoofing" occurs when a caller deliberately falsifies the information transmitted to the called party's Caller ID

(continued….)

III. DISCUSSION

A. Caller ID Exemption for Threatening Calls

7. *The Need for an Exemption*. We modify our Caller ID rules to exempt threatening calls from the CPN privacy rules so that security personnel and law enforcement have quick access to information they need to aid their investigations. We agree with the vast majority of commenters that the exemption promotes public safety.[21] AT&T, for example, "strongly supports" an additional exemption under the Caller ID rules, saying that blocked Caller ID "may impede law enforcement investigations of threatening calls and hinder responses to these threats."[22] The record shows that even when a threatening call proves to be a hoax, it can nonetheless result in substantial disruption and expenditure of public resources by law enforcement.[23] Moreover, one party argues that a permanent amendment to the rules outlining how blocked Caller ID information can be disclosed would "permit[] law enforcement agencies to know with certainty what their investigative rights and responsibilities will be when their constituents are threatened."[24]

8. The need for the exemption is illustrated by reports of widespread and increasing numbers of threatening calls that have targeted schools, religious organizations, and other entities. One recent study found that the incidents of bomb threats made to schools from 2011-16 increased by 1,461 percent, and that more than half of such threats were made by phone.[25] Similarly, a 2016 report from the Bureau of Alcohol, Tobacco, Firearms and Explosives describes a substantial increase in bomb threats to schools and residences.[26] Media reports confirm this disturbing trend.[27] Although the record does not indicate how often threatening callers use the privacy indicators required by section 64.1601(b), parties seeking waiver of the rule have asserted that they frequently do so.[28]

(Continued from previous page)
display to disguise their identity. Spoofing is often used to trick the called party into giving away valuable personal information so it can be used in fraudulent activity. Federal law prohibits spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value. 47 U.S.C. § 227(e)(1); *see also* 47 CFR § 64.1604(a); Federal Communications Commission, Spoofing and Caller ID, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id (last visited Sept. 19, 2017). We are addressing Caller ID spoofing in other proceedings. *In the Matter of Call Authentication Trust Anchor*, Notice of Inquiry, Docket No. 17-97 (2017); *see also* AT&T Aug. 21, 2017 Comments at 6-7; Louis Taff Aug. 16, 2017 Comments at 2.

[21] Comments filed in response to the recent waiver request from Jewish Community Centers have suggested that the Commission broaden the scope to allow law enforcement to obtain the Caller ID of any threatening caller. *See* TDR Technologies Mar. 17 Comments at 3; Shira Fischer Mar. 17 Comments; Rachel Mar. 17 Comments ("If someone is making a threat to the life or physical safety of someone else, they should not be able to benefit from telephone privacy protections.").

[22] AT&T Aug. 21, 2017 Comments at 1; *see also* Hatzalah Aug. 21, 2017 Comments at 3.

[23] *See Middletown Petition* at 5.

[24] E-Rate Aug. 21, 2017 Comments at 2.

[25] *See* Dr. Amy Klinger and Amanda Klinger, Esq., Bomb Incidents in Schools: An Analysis of 2015-16 School Year, http://eschoolsafety.org/bir-2016/ (last visited Sept. 27, 2017).

[26] *See* ATF Report: https://www.atf.gov/resource-center/docs/bomb-threats-across-us/download (finding an 84% increase in bomb threats to schools from 2010-2016 and a 184% increase in bomb threats to residences from 2013-14).

[27] *See supra* n.1.

[28] *See*, *e.g.*, *Petition of National Aeronautics and Space Administration for Waiver of Federal Communications Commission Regulations at 47 C.F.R. 64.1601(b)* at 3 (filed Nov. 6, 2006) (confirming that "parties perpetrating these calls often use the CPN restrictions in order to prevent authorities from timely identifying their location"); *Petition of Liberty Public School District for Waiver of Federal Communications Commission Regulations at 47*
(continued….)

9. This new exemption is consistent with the Commission's prior approach in this area. The Commission has previously concluded, for example, that to the extent Caller ID services are used to deliver emergency services, privacy requirements should not apply to delivery of CPN to a public agency's emergency lines, a poison control line, or in conjunction with 911 emergency services.[29] In these instances, the Commission concluded that Caller ID blocking mechanisms could jeopardize emergency services and therefore pose a serious threat to safety. We believe that threatening calls present equally compelling circumstances in which the need to ensure public safety, in accordance with the Commission's fundamental statutory mission,[30] outweighs any CPN privacy interest of the threatening caller.

10. We disagree with the sole commenter who urges us to not adopt an exemption but instead continue to issue case-by-case waivers, albeit on a streamlined basis.[31] The waiver process, even if streamlined, would not provide equivalent benefits in combatting threatening calls. Investigation of these cases can depend on immediate action to stop a potentially catastrophic event.[32] An exemption would allow for virtually immediate access to blocked Caller ID information upon proper request in threatening situations. We thus agree with the commenters who point out that threatening calls should be addressed immediately through an exemption in our rules rather than a case-by-case waiver process.[33]

11. We also disagree with commenters who urge that carriers should have discretion to decline law enforcement requests to get Caller ID information.[34] CTIA claims that a mandate is not necessary, noting both the industry's long and successful track record of cooperation with law enforcement and that the Electronic Communications Privacy Act (ECPA)[35] utilizes a voluntary disclosure provision.[36] While we believe that the industry's record may indeed be laudatory, we conclude that mandatory disclosure is essential to our exemption.[37] The record reveals no scenarios where a

(Continued from previous page)
C.F.R. 64.1601(b) at 5 (filed Apr. 22, 2007) (confirming use of CPN restrictions by threatening callers); *Middletown Petition* at 5.

[29] 47 CFR § 64.1601(d); *Caller ID Order*, 9 FCC Rcd at 1770, para. 37.

[30] *See* 47 U.S.C. § 151 (creating the FCC "[f]or the purpose of regulating interstate and foreign communication … so as to make available . . . a . . . communication service . . . for the purposes of promoting safety of life and property through the use of wire and radio communications").

[31] CTIA Aug. 21, 2017 Comments at 11.

[32] *See* E-Rate Aug. 21, 2017 Comments ("A late waiver may ultimately lead to the [perpetrator] of the threatening calls, but only after the immediate threat has abated — or, worse yet, has been carried out."); *see also supra* n.2.

[33] *See* AT&T Aug. 21, 2017 Comments at 3 ("the Commission properly recognizes the importance of ensuring that these rules do not hinder law enforcement in addressing threatening calls"); E-Rate Aug. 21, 2017 (proposed rule change would eliminate time-consuming and burdensome case-by-case waiver process, and stated Liberty Public School had 2,209 elapsed days between request and grant of a waiver, Chevrah Hatzalah Volunteer Ambulance Corps had 509 elapsed days, Enlarged City School District of Middletown had 55 elapsed days, and Jewish Community Centers had 3 elapsed days).

[34] CTIA Aug. 21, 2017 Comments at 6; NTCA – The Rural Broadband Association Sept. 19, 2017 Reply Comments at 2 (NTCA Reply Comments); AT&T Aug. 21, 2017 Comments at 4; CenturyLink Sept. 19, 2017 Reply Comments at 2.

[35] 18 U.S.C. § 2702(c)(4).

[36] CTIA Aug. 21, 2017 Comments at 6; NTCA – The Rural Broadband Association Sept. 19, 2017 Reply Comments at 2 (NTCA Reply Comments). *Compare* 18 U.S.C § 2702(c)(4) (a provider may disclose a record or other information pertaining to a subscriber under the circumstances set forth) *with id.* § 2703 (contains required disclosures).

[37] We decline to define a "valid request" from law enforcement, as suggested by CenturyLink, because CTIA states carriers have an excellent track record of complying with law enforcement requests under ECPA. CenturyLink, Inc. (continued….)

request for Caller ID by law enforcement, as we describe below, should give carriers reason to question the validity of the emergency. Further, the imminent and grave nature of threatening calls, as defined below, leave little time for the exercise of discretion in *whether* to disclose information after law enforcement has become involved.[38]

12. We agree with AT&T that carriers should not be subject to liability for violation of our Caller ID privacy rules if they disclose blocked Caller ID pursuant to our new exemption.[39] As CTIA notes, "[l]aw 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."[40] Law enforcement's determination of a threatening call coupled with the mandatory nature of the disclosure removes any justification for placing liability on carriers who comply with a proper request for blocked Caller ID.[41] To the extent that AT&T and NTCA ask the Commission to somehow exempt carriers from any other legal liability, we decline to do so.[42] Our concern is only with ensuring that Commission rules do not interfere with the ability of carriers to respond to law enforcement requests as allowed under law.

13. *Definition of "Threatening Call."* We define the term "threatening call," which triggers the application of the new exemption, as "any call that conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency."[43] This definition ensures consistency with the emergency-disclosure provision of ECPA,[44] as urged by several commenters, and because it satisfies our goal of targeting the most threatening calls.[45]

(Continued from previous page)
Sept. 19, 2017 Reply Comments at 3 (CenturyLink Reply Comments); CTIA Aug. 21, 2017 Comments at 11. We decline at this time to create a new law enforcement request process because the record reveals no evidence that law enforcement requests for this information have been ineffective or unreliable in the past.

[38] As discussed below, we adopt the ECPA standard for disclosure of information. We do not find that standard to be inconsistent with a mandatory disclosure requirement. Carriers that are required to make disclosures in the very specific, narrowly defined scenario covered by our new exemption will not violate the more flexible ECPA standard by complying with our requirement. Moreover, we believe that a law enforcement request based on the possibility of death or serious injury can satisfy ECPA's "good faith" standard to justify a carrier's voluntary disclosure of such information.

[39] AT&T Aug. 21, 2017 Comments at 6.

[40] CTIA Aug. 21, 2017 Comments at 9.

[41] CTIA suggests that we adopt a provision stating that section 64.1601(b)'s prohibition on 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." Such a provision is unnecessary in light of our existing rule, section 64.1601(d)(4)(iii), exempting "legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency." CTIA Aug. 21, 2017 Comments at 12; 47 CFR § 64.1601(d)(4)(iii); CenturyLink Sept. 19, 2017 Reply Comments at 3.

[42] AT&T Aug. 21, 2017 Comments at 6; *see also* NTCA Sept. 19, 2017 Reply Comments at 3-4 (stating "any amendments should also include "safe harbor" provisions for carriers acting in good faith who, under time-sensitive circumstances (and especially in remote areas and under extraordinary conditions, such as snowstorms, natural disasters, etc.), may find it imperative to divulge blocked Caller ID information to called parties, volunteer rescuers, or similar non-law enforcement personnel"). We address NTCA's request, which concerns who may receive the Caller ID information rather than who may request the Caller ID information, in n.61, *infra.*

[43] Typically, a call from a person simply reporting a threat, where the facts of the call indicate that the caller wishes to remain anonymous, would not be subject to disclosure because disclosure would not be necessary to prevent death or serious bodily injury. In the event disclosure is necessary to prevent death or serious bodily injury, however, the rule would allow disclosure only to law enforcement. We think this is appropriate and permitted by ECPA's emergency exception. We do not wish to deter anonymous tips made to law enforcement.

[44] 18 U.S.C. § 2702(c)(4) ("A provider . . . may divulge a record or other information pertaining to a subscriber to or customer of such service . . . to a governmental entity, if the provider, in good faith, believes that an emergency
(continued….)

14. In the *Caller ID NPRM*, we proposed to define a "threatening call" as "any call that includes a threat of serious and imminent unlawful action posing a substantial risk to property, life, safety, or health."[46] Commenters urge that the Commission align its definition with ECPA's emergency-disclosure exception, noting that our proposed definition is inconsistent with ECPA, and might be either over or under-inclusive depending on the circumstances.[47] ECPA, in relevant part, states that a provider ". . . may divulge a record or other information pertaining to a subscriber to or customer of such service . . . to a governmental entity, 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."[48] CTIA notes that the Commission's proposed definition would require disclosure of caller information in circumstances where existing federal law does not currently permit, such as a call threatening to steal a car.[49] We agree that our rule should be closely tailored to the scope of ECPA's emergency-disclosure exception.

15. Because carriers are already familiar with the ECPA standard and ECPA covers the imminent nature of the dangers envisioned by the *Caller ID NPRM* and commenters, we tailor our rule to align with the ECPA definition for purposes of this new exemption.[50] We agree that it makes sense to align our definition of a threatening call with existing federal law to ensure that carriers have consistent legal standards to apply in situations where both our rules and ECPA apply. We also agree with commenters that the ECPA definition would sufficiently cover the types of calls we seek to exempt from the Caller ID blocking rule, without being either over- or under-inclusive, or including terms that could be ambiguous.[51]

16. *Law Enforcement Involvement*. We find that, to ensure the exemption is not abused, a request for blocked Caller ID information associated with a threatening call must be made by law enforcement on behalf of the threatened party. We believe that this requirement will, among other things, ensure that such requests concern a *bona fide* threatening call and will not be a pretext for obtaining blocked Caller ID for other purposes. As CTIA commented, such a requirement will ensure there is no

(Continued from previous page)
involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."); CenturyLink Sept. 19, 2017 Reply Comments at 2.

[45] NCTA states that 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.'" NCTA Sept. 19, 2017 Reply Comments at 3. We decline to use NCTA's definition because referring to "emergency" rather than to "threat" encompasses more situations where immediate disclosure is necessary to address an emergency. Additionally, our proposed definition is consistent with ECPA. 18 U.S.C. § 2702(c)(4). Finally, we include "disclosure without delay" within the definition to further align the FCC's disclosure requirement under circumstances where ECPA allows it. 18 U.S.C. § 2702(c)(4).

[46] *Caller ID NPRM* at para 12.

[47] AT&T Aug. 21, 2017 Comments at 1; CTIA Aug. 21, 2016 Comments at 5-6; NTCA Sept. 19, 2017 Reply Comments at 2; CenturyLink Sept. 19, 2017 Reply Comments at 2; NCTA Sept. 19, 2017 Reply Comments at 3.

[48] 18 U.S.C. § 2702(c)(4).

[49] *See* CTIA Aug. 21, 2017 Comments at 6-7.

[50] *See* 18 U.S.C. § 2702(c)(4).

[51] Louis Taff suggests eliminating the words "serious," imminent" and "substantial" from the Commission's proposed definition, noting that, for example, a call threating that "a city council meeting will be blown up exactly one year from today" might not be considered "imminent," while still clearly posing a threat. Louis Taff Aug. 16, 2017 Comments at 1. Taff's suggestions are mooted by the ECPA-based changes in our adopted definition, which are consistent with his suggestions.

ambiguity regarding the necessary level of law enforcement involvement.[52]

17. We agree with commenters that law enforcement involvement at this stage of the process is essential to avoid having carriers make a determination on what constitutes a threatening call.[53] AT&T avers that the involvement of law enforcement would help ensure compliance with the ECPA disclosure requirements,[54] and would help prevent overbroad disclosures of blocked caller ID information that may harm the privacy of non-threatening callers.[55] According to AT&T, law enforcement officials are "indisputably better qualified to validate the existence of emergency circumstances than carrier personnel," and are likely more familiar with the facts giving rise to a requested disclosure.[56] CTIA adds that requiring law enforcement involvement when restricted Caller ID information is requested would deter parties from manipulating the unblocking process.[57] We agree with commenters that law enforcement personnel are in the best position to determine the existence of a credible threat that necessitates revealing CPN to investigate the threatening call.

18. Likewise, we find that only law enforcement personnel and, as directed by law enforcement, others directly responsible for the safety and security of the threatened party should *receive* the otherwise protected Caller ID information in the case of threatening calls.[58] Security personnel may only receive the blocked Caller ID information from the providers as directed by law enforcement because law enforcement will generally be in a better position than providers to determine who qualifies as security personnel.[59] We limit the disclosure of the blocked Caller ID information to prevent abuse,[60] and to protect the privacy interests of parties who may block their Caller ID for valid privacy interests, such as domestic violence victims. By limiting the disclosure to law enforcement or, as directed by law enforcement, to security personnel for purposes of investigating a threat, we seek to prevent exploitations of the amended rule, such as an abuser tracking down a victim. We define security personnel as "those individuals directly responsible for maintaining safety of the threatened entity consistent with the nature of the threat."[61] We allow disclosure to security personnel as directed by law enforcement to encompass

[52] *See* Letter from Melanie K. Tiano, Director, CTIA, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 91-281, at 2 (filed Oct. 16, 2017) (CTIA *Ex Parte*).

[53] *See* AT&T Aug. 21, 2017 Comments at 4-6; CTIA Aug. 21, 2017 Comments at 7-10; NCTA Sept. 19, 2017 Reply Comments at 2; CenturyLink Sept. 19, 2017 Reply Comments at 2; CTIA *Ex Parte* at 2.

[54] AT&T Aug. 21, 2017 Comments at 4-5 ("To avoid creating any such conflicting obligations under Commission rules and the ECPA, the Commission should remove the proposed definition of 'threatening calls' and modify the proposed exception to Rule 64.1601(b) to be expressly consistent with Section 2702(c)(4) of the ECPA. Specifically, the new exception to the Caller ID privacy rules should state that the privacy indicator for blocked Caller ID information does not apply where such information is the subject of a lawful request by a law enforcement agency as authorized by 18 U.S.C. § 2702(c)(4).").

[55] *See id.* at 4-6.

[56] *Id*. at 5-6. AT&T states that carrier determination of what is a threatening call could lead to significant costs and burdens associated with hiring personnel with law enforcement experience, and that carriers would also need expertise in how to avoid giving Caller ID information to those that seek to mislead the carrier to obtain restricted Caller ID information for illicit purposes. *Id*.

[57] CTIA Aug. 21, 2017 Comments at 7-10.

[58] *See infra* n.61 for examples of who may qualify as security personnel for purposes of this exemption.

[59] CTIA *Ex Parte* at 2 ("Alternatively, if the Commission perceives a need for carriers to provide information to security personnel the rules should make it clear that the information should be provided '**as directed by law enforcement.**'" (emphasis in original)).

[60] *See id.* at 9; NCTA Sept.19, 2017 Reply Comments at 3-4; CenturyLink Sept. 19, 2017 Reply Comments at 2.

[61] For example, employees whose duties include security at an institution would qualify as security personnel; by contrast, an employee who merely answered the threatening phone or an individual homeowner would not. Security personnel may include, but are not limited to, corporate and government agency security personnel, and school or (continued….)

situations where security personnel need access to the blocked Caller ID information for investigative purposes, as in instances when a large institution with its own security force, like a university or government agency, receives a threat.[62]

19. We agree with CTIA's recommendation that "called parties should not be the recipients of information," and the "use of disclosed CPN should be restricted – by rule – in a manner consistent with prior waivers."[63] Accordingly, we include the following conditions in our rule for law enforcement or, as directed by law enforcement, security personnel of the called party investigating the threat: (1) the CPN on incoming restricted calls may not be passed on to the line called; (2) any system used to record CPN must be operated in a secure way, limiting access to designated telecommunications and security personnel, as directed by law enforcement; (3) telecommunications and security personnel, as directed by law enforcement, may access restricted CPN data only when investigating calls involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency, and shall document that access as part of the investigative report; (4) carriers transmitting restricted CPN information must take reasonable measures to ensure the security of such communications;[64] (5) CPN information must be destroyed in a secure manner after a reasonable retention period; and, (6) any violation of these conditions must be reported promptly to the Commission. We expect that these boundaries on how the disclosed Caller ID information must be treated will advance public safety efforts while protecting valid privacy interests. We have imposed these conditions on waivers both to ensure that the Caller ID information in question is accessible only to persons with direct involvement in investigating the threatening calls and to ensure that the information is used only for that purpose.[65] We have no indication that these conditions did not properly protect privacy interests in the cases underlying the waivers, and the record does not reveal any reason to doubt their efficacy more generally.[66]

20. *Carrier Obligations Under Section 222.* We find that the disclosure required by the new exemption we adopt here is consistent with section 222 of the Act. Section 222(a) states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications

(Continued from previous page)
university security staff acting within the scope of their duties. In the case of an individual homeowner, law enforcement can take reasonable action to protect the homeowner as it conducts its investigation of a threatening call.

[62] CTIA *Ex Parte* at 2; *see NASA Order*, 27 FCC Rcd at 507 ("NASA notes that [John F. Kennedy Space Center] provides both the security service and end office telecommunications to all locations within its geographic boundaries").

[63] *Id.* at 10; *see also* AT&T Aug. 21, 2017 Comments at 9-10. In its reply comments, NTCA asserts that, in times of exigency or in remote or insular areas, Caller ID information should be available to volunteer rescuers and similar non-law enforcement personnel with a safe harbor provision for carriers. NTCA Reply Comments at 3-4. The rules we adopt here make Caller ID information available to "security personnel," as directed by law enforcement, as well as law enforcement, and our definition of "security personnel" does not necessarily exclude the types of situations NTCA describes. The determination NTCA urges would dependent on the facts of a specific situation, and is, therefore, not appropriate for the general exemption we adopt here.

[64] CTIA *Ex Parte* at 3.

[65] *Rules and Policies Regarding Calling Number Identification Service – Caller ID*, *Waiver of Federal Communications Commission Regulations at 47 CFR 64.1601(b) on Behalf of Jewish Community Centers*, CC Docket No. 91-281, Temporary Waiver Order, 32 FCC Rcd 1559, at 1563, para. 10 (CGB 2017) (*JCC Temporary Waiver Order*); *Middletown Waiver*, 31 FCC Rcd at 3569-70; *Liberty School Order*, 28 FCC Rcd at 6416.

[66] *JCC Temporary Waiver Order*, 32 FCC Rcd at 1563, para. 10.

carrier."[67] Our amended rule requiring carriers to disclose blocked Caller ID information when law enforcement requests it to investigate threatening calls does not contravene carriers' obligations under section 222.

21. In addressing the threatening calls recently received by Jewish Community Centers, the Bureau discussed section 222 in connection with the statutory protection of customer proprietary network information.[68] We agree with the Bureau's view that section 222(d) allows for carriers to disclose blocked Caller ID in the case of unlawful activity because section 222(d) states, "[n]othing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents . . . to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[69] As described above, we define a "threatening call" as "any call that conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency." By limiting the disclosure of blocked Caller ID to narrowly defined cases of threatening calls that raise the "danger of death or serious physical injury to any person," we ensure that carriers are within their obligations under section 222.

B. The Jewish Community Centers' Temporary Waiver

22. On February 28, 2017, Senator Charles E. Schumer submitted a letter to the Commission expressing concern regarding recent bomb threats made via phone against various Jewish Community Centers (JCCs) in New York and across the nation.[70] Senator Schumer noted that the Commission has played a valuable role in ensuring law enforcement and others are not hindered in their access to the caller information of threatening calls and suggested consideration of the grant of a waiver.[71] On March 3, 2017, CGB granted to JCCs, and any carriers that serve JCCs, a temporary, emergency waiver of section 64.1601(b) of the Commission's rules.[72] In so doing, CGB indicated that this temporary waiver would remain in effect until the Commission determined whether the waiver should be made permanent.[73] In addition, CGB sought comment on whether to make this waiver permanent.[74] Comments filed in response support the waiver[75] and note the public interest in promoting efforts to identify and thwart individuals making threatening calls to JCCs.[76] No commenter opposed the waiver.

23. In the *Caller ID NPRM*,[77] the Commission confirmed that good cause continued to exist

[67] 47 U.S.C. § 222(a).

[68] *JCC Temporary Waiver Order*, 32 FCC Rcd at 1563, n.35.

[69] 47 U.S.C. § 222(d)(2).

[70] *See* Letter from Senator Charles E. Schumer to Chairman Ajit Pai, FCC, dated Feb. 28, 2017 (Schumer Letter).

[71] *Id.*

[72] *See JCC Temporary Waiver Order*, 32 FCC Rcd at 1559, para. 1.

[73] *Id*. at 1564, para. 12.

[74] *See Consumer and Governmental Affairs Bureau Seeks Comment on Waiver Regarding Access to Calling Party Numbers Associated with Threatening Phone Calls Made to Jewish Community Centers*, CC Docket No. 91-281, Public Notice, 32 FCC Rcd 1556, para. 1 (CGB 2017).

[75] *See, e.g.*, AT&T Services Mar. 17, 2017 Comments at 2; Shira Fischer Mar. 17, 2017 Comments; TDR Technology Mar. 20, 2017 Comments (suggesting that the scope of the waiver be broadened to include schools and other religious institutions).

[76] *See* AT&T Services Mar. 17, 2017 Comments at 2-4 ("a permanent waiver of Rule 64.1601(b) prohibiting the overriding of the caller ID privacy indicator is clearly necessary to protect JCCs in light of the recent threats described by Senator Schumer and is fully justified by the Commission's rules and precedent").

[77] *Caller ID NPRM* at para. 19.

to maintain the temporary waiver of section 64.1601(b) granted to JCCs and the carriers who serve them for disclosure of CPN associated with threatening calls.[78] The *Caller ID NPRM* stated that in the event the Commission were to amend its rules to recognize a more general exemption for threatening calls, the JCC waiver would be encompassed within the protections afforded by that exemption.[79] With this *Report and Order,* we recognize an exemption for threatening calls thereby encompassing the JCC waiver. Accordingly, the JCC waiver is no longer necessary, and is superseded by this order and terminated as of the effective date of the rule changes adopted herein.

C. Exemption for Non-Public Entities Providing Emergency Services.

24. We also amend our rules to allow non-public emergency services to receive the CPN of all incoming calls from blocked numbers requesting assistance. We believe amending our rules to allow non-public emergency services access to blocked Caller ID promotes the public interest by ensuring timely provision of emergency services without undermining any countervailing privacy interests.[80]

25. The Commission previously concluded that "[t]o the extent that CPN-based services are used to deliver emergency services, we find that privacy requirements for CPN-based services should not apply to delivery of the CPN to a public agency's emergency line, a poison control line, or in conjunction with 911 emergency services"[81] and has noted that "in an emergency, a caller is not likely to remember to dial or even know to dial an unblocking code."[82] Here we take the Commission's previous conclusions a logical step further by amending the rules to allow non-public emergency services to retrieve from carriers the blocked Caller ID of callers seeking assistance. We believe these callers would want an emergency service, whether a public agency or non-public entity, to be able to quickly and easily contact or locate them using their phone number to provide assistance.

26. The Bureau previously waived the Caller ID privacy rule for a private ambulance service,[83] Chevrah Hatzalah Volunteer Ambulance Corps Inc. (Hatzalah).[84] In granting the waiver, the Bureau noted that Hatzalah's automatic dial retrieval system ". . . is disrupted when the incoming call comes from a caller who has requested that his/her number not be revealed to the called party. In this circumstance, Hatzalah states that the inability to automatically identify callers creates several problems that can delay or even prevent the timely provision of emergency care."[85] In its petition, Hatzalah further argued that allowing it to access blocked Caller ID information "would not frustrate [the] purpose [of the Commission's rule] because the Commission has recognized that a caller's privacy interest should not interfere with the delivery of emergency services."[86]

27. The Bureau found that the waiver served the public interest "because Hatzalah will be better able to respond to emergency situations by saving the crucial time taken when requesting phone

---

[78] 47 U.S.C. § 151.

[79] *Caller ID NPRM* at para. 19.

[80] *See Hatzalah Order*.

[81] *Caller ID Order*, 9 FCC Rcd at 1770, para. 37; *see also* 47 CFR § 64.1601(d)(4)(ii). In addition, our rules exempt "legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency." 47 CFR § 64.1601(d)(4)(iii).

[82] *Caller ID Order*, 9 FCC Rcd at 1771, para. 43.

[83] *Hatzalah Order*, 28 FCC Rcd at 1253, para. 1.

[84] *See Petition of Chevrah Hatzalah Volunteer Ambulance Corps Inc., for Waiver of § 64.1601(b) Regarding the Transmission of Calling Party Number*, CC Docket No. 91-281 (filed on Sept. 30, 2011) (*Hatzalah Petition*).

[85] *Id*.

[86] *Hatzalah Order*, 28 FCC Rcd at 1255, para. 7 (citing *Hatzalah Petition* at 6-7).

number and location information from the caller."[87] The Bureau also noted, ". . . people seeking emergency services are often under great stress when they call, which can lead to difficulty in accurately communicating the vital telephone number and location information."[88] Finally, the Bureau agreed with Hatzalah "that a caller seeking emergency services has an interest in the number becoming known to the emergency provider to speed the provision of emergency services and, therefore, any privacy concerns are minimized in this context."[89]

28. In the *Caller ID NPRM*, the Commission sought comment on whether it should extend the proposed exemption to non-public entities that provide emergency services such as private ambulance companies. Hatzalah urges us to amend our rules for the same reasons the Bureau granted it a waiver so that other non-public emergency services will also have access to blocked Caller ID to provide the requested assistance. We agree that the *Hatzalah Order's* reasoning should apply more generally and find that allowing non-public emergency services to access blocked Caller ID promotes public safety and does not undermine any countervailing privacy interests associated with revealing CPN.[90] In order to facilitate the public safety goals of non-public emergency services, we amend our Caller ID privacy rules to allow such services to obtain blocked Caller ID from carriers.

29. Consistent with the *Hatzalah Order*,[91] entities providing emergency services must be licensed by a state or municipality to provide such services to qualify for this exemption.[92] Unlike the threatened callers discussed above, non-public emergency services do not have to act in conjunction with law enforcement to obtain blocked Caller ID information from carriers. Involving public emergency services in this scenario would undermine the goal of allowing providers of emergency services to provide quick and effective assistance to individuals seeking such assistance.

IV. PROCEDURAL MATTERS

A. Regulatory Flexibility Act Analysis

30. Pursuant to the Regulatory Flexibility Act of 1980, as amended,[93] the Commission's Final Regulatory Flexibility Analysis in this Report and Order is attached as Appendix C.

B. Paperwork Reduction Act

31. This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

C. Congressional Review Act

32. The Commission will send a copy of this Report and Order to Congress and the

[87] *Id.*at 1258, para. 11 (citing *Hatzalah Petition* at 3).

[88] *Id.*

[89] *Id.* at 1259 para. 11.

[90] *See Hatzalah Reply Comments at 4.*

[91] *See Hatzalah Order*, 28 FCC Rcd at 1255, para. 5.

[92] *See* Hatzalah Reply Comments at 1 (stating "Hatzalah is the only volunteer ambulance service licensed to serve the entire City of New York.").

[93] *See* 5 U.S.C. § 603.

Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

D. Materials in Accessible Formats

33. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

V. ORDERING CLAUSES

34. **IT IS ORDERED**, that, pursuant to the authority contained in Sections 1-4, 201 and 222 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201, 222 this *Report and Order* **IS ADOPTED** and that Part 64 of the Commission's rules, 47 CFR §§ 64.1600, 64.1601, are amended as set forth in Appendix A. These sections, which contain new or modified information collection requirements that require review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA), shall become effective 30 days after the Commission's publication of a notice in the *Federal Register*, which will announce approval by OMB under the PRA.

35. **IT IS FURTHER ORDERED** that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, **SHALL SEND** a copy of this *Report and Order* to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

36. **IT IS FURTHER ORDERED** that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, **SHALL SEND** a copy of this *Report and Order*, including the Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends part 64 of Title 47 of the Code of Federal Regulations (CFR) as follows

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. Amend Section 64.1600 by adding new paragraph (1) to read as follows

§ 64.1600 Definitions.

* * * * *

(l) *Threatening Call*. The term "threatening call" is any call that conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency.

2. Amend section 64.1601 by revising paragraph (d)(4)(ii) to read as follows, and by adding new paragraph (f) and (g) to read as follows:

§ 64.1601 Delivery requirements and privacy restrictions.

* * * * *
(d) * * * * *
(4) * * * * *
(ii) Is used on a public agency's emergency telephone line or in conjunction with 911 emergency services, on a telephone line to contact non-public emergency services licensed by the state or municipality, or on any entity's emergency assistance poison control telephone line; or
* * * * *
(f) Section 64.1601(b) shall not apply when CPN delivery is made in connection with a threatening call. Upon report of such a threatening call by law enforcement on behalf of the threatened party, the carrier will provide any CPN of the calling party to law enforcement and, as directed by law enforcement, to security personnel for the called party for the purpose of identifying the party responsible for the threatening call.
(g) For law enforcement or security personnel of the called party investigating the threat:
(1) the CPN on incoming restricted calls may not be passed on to the line called;
(2) any system used to record CPN must be operated in a secure way, limiting access to designated telecommunications and security personnel, as directed by law enforcement;
(3) telecommunications and security personnel, as directed by law enforcement, may access restricted CPN data only when investigating phone calls of a threatening and serious nature, and shall document that access as part of the investigative report;
(4) carriers transmitting restricted CPN information must take reasonable measures to ensure security of such communications;
(5) CPN information must be destroyed in a secure manner after a reasonable retention period; and
(6) any violation of these conditions must be reported promptly to the Commission.

APPENDIX B

Comments Filed

Commenter	Abbreviation
AT&T Services, Inc.	AT&T
Chevrah Hatzalah Volunteer Ambulance Corps Inc.	Hatzalah
CenturyLink, Inc.	**CenturyLink**
CTIA	CTIA
E-Rate Central	E-Rate
NCTA – The Internet & Television Association	**NCTA**
NTCA – The Rural Broadband Association	**NTCA**
Chris Kiefer	Kiefer
Bradley Ponce	Ponce
Sabrina Scott	Scott
Louis Taff	Taff

* Bold – reply comments only.

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980 (RFA),[1] as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Notice of Proposed Rulemaking* (*NPRM*).[2] The Commission sought written public comment on the proposals in the *NPRM*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Order

2. This *Report and Order* takes an important step to help security and law enforcement personnel responsible for the safety of parties receiving certain threatening calls obtain quick access to the Caller ID information needed to identify and thwart threatening callers. In recent years, media and law enforcement reports indicate that the number of threatening calls appears to be increasing dramatically.[4] These calls result in substantial disruption among schools, religious organizations, and other entities, which has traumatized communities and left schoolchildren fearful. These threats also drain public resources by requiring the deployment of police and bomb units in response. Schools and others receiving threats have suggested that blocked Caller ID hinders a rapid response. The *Report and Order* moves away from case-by-case waivers to the streamlined approach necessary to help protect the safety of threatened parties in a timely way. Specifically, the *Report and Order* clears the way for carriers to disclose blocked Caller ID information associated with threatening calls to facilitate the investigation of such threats and amends our rules to allow non-public emergency services to obtain blocked Caller ID information associated with calls requesting assistance.

3. *Caller ID Exemption for Threatening Calls*. The *Report and Order* modifies our Caller ID rules to exempt threatening calls from the CPN privacy rules, so that security personnel and associated law enforcement have quick access to information they need to aid their investigations.[5] The *Report and Order* defines the term "threatening call," which triggers the application of the new exemption, as "any call that conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency."[6] This definition is consistent with the emergency-disclosure provision of ECPA,[7] and it satisfies our goal of targeting the most threatening calls.[8]

---

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612 has been amended by the Contract With America Advancement Act of 1996, Public Law No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[2] *Rules and Policies Regarding Calling Number Identification Service — Caller ID*, CC Docket No. 91-281, Notice of Proposed Rulemaking, FCC 17-76 (June 22, 2017) (*Caller ID NPRM*).

[3] *See* 5 U.S.C. § 604.

[4] *See Caller ID NPRM* at para. 2.

[5] *Report and Order* at para. 7.

[6] *Id.* at para. 13.

[7] 18 U.S.C. § 2702(c)(4) ("A provider…may divulge a record or other information pertaining to a subscriber to or customer of such service… to a governmental entity, 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.").

[8] *Report and Order* at para. 13.

4. *Law Enforcement Involvement*. To ensure the exemption is not abused, a request for blocked Caller ID associated with a threatening call must be made by law enforcement on behalf of the threatened party.[9] We believe that this requirement will, among other things, ensure that such requests concern a *bona fide* threatening call and will not be a pretext for obtaining blocked Caller ID for other purposes.[10]

5. *Only Law Enforcement and Security Personnel Receive Blocked Caller ID*. Only law enforcement personnel and others responsible for the safety and, as directed by law enforcement, security personnel of the threatened party should *receive* the otherwise protected Caller ID information in the case of threatening calls.[11] The *Report and Order* limits the disclosure of the blocked Caller ID information to prevent abuse of the disclosure process,[12] and to protect the privacy interests of parties who may block their Called ID for valid privacy interests, such as domestic violence victims.[13] The *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."[14]

6. *Conditions on Receipt of Blocked Caller ID Information*. The *Report and Order* includes the following conditions in our rule for law enforcement or security personnel of the called party investigating the threat: (1) the CPN on incoming restricted calls may not be passed on to the line called; (2) any system used to record CPN must be operated in a secure way, limiting access to designated telecommunications and, as directed by law enforcement, security personnel; (3) telecommunications and, as directed by law enforcement, security personnel may access restricted CPN data only when investigating calls involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency, and shall document that access as part of the investigative report; (4) carriers transmitting restricted CPN information must take reasonable measures to ensure the security of such communications; (5) CPN information must be destroyed in a secure manner after a reasonable retention period; and (6) any violation of these conditions must be reported promptly to the Commission.[15]

7. *Carrier Obligations Under Section 222.* The disclosure required by the new exemption adopted in the *Report and Order* is consistent with section 222 of the Act. Section 222(a) states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[16] Our amended rule requiring carriers to disclose blocked Caller ID information when law enforcement requests it does not contravene carriers' obligations under section 222.[17]

---

[9] *Report and Order* at para. 16.

[10] *Id.* at para. 16.

[11] *Id.* at para. 18.

[12] CTIA Aug. 21, 2017 Comments at 9.

[13] *Report and Order* at para. 18.

[14] For example, dedicated employees tasked with security at an institution would qualify as security personnel, as opposed to a non-security tasked employee that answered the phone call that conveyed the threat, or an individual homeowner. In the case of an individual homeowner, law enforcement can take reasonable action to protect the homeowner as it conducts its investigation of a threatening call. *Report and Order* at para. 18.

[15] *Report and Order* at para. 19.

[16] 47 U.S.C. § 222(a); *Report and Order* at para. 20.

[17] *Report and Order* at para. 20.

8. *Jewish Community Center Temporary Waiver*. The *Report and Order* recognizes an exemption for threatening calls thereby encompassing the JCC waiver.[18] Accordingly, the JCC waiver is no longer necessary, and is superseded by the *Report and Order*.[19]

9. *Non-Public Emergency Services*. The *Report and Order* also amends our rules to allow non-public emergency services to receive the CPN of all incoming calls from blocked numbers requesting assistance.[20] Amending our rules to allow non-public emergency services access to blocked Caller ID promotes the public interest by ensuring timely provision of emergency services without undermining any countervailing privacy interests.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

10. In the *NPRM*, we solicited comments on how to minimize the economic impact of our proposals on small businesses. While commenters did not directly reference the IRFA, two of the commenters addressed the area of duplicate, overlapping, or conflicting rules,[21] and three addressed the burden on all carriers in determining what constitutes a "threatening call."[22] None of the comments pointed out any areas where small business would incur a particular hardship in complying with the rules.

11. *Rules Should Be Consistent with the Electronic Communications Privacy Act (ECPA)*. AT&T and CTIA urge that the Commission align its definition with the ECPA's emergency-disclosure exception to avoid conflicting rules.[23] ECPA, in relevant part, states that a provider ". . . may divulge a record or other information pertaining to a subscriber to or customer of such service . . . to a governmental entity, 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."[24] We agree that our rule should be closely tailored to the scope of ECPA's emergency-disclosure exception.[25] We define the term "threatening call," which triggers the application of the new exemption, as "any call that conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency."[26]

12. *Law Enforcement Should Validate Circumstances Surrounding Disclosure of Blocked Caller ID.* AT&T avers that the involvement of law enforcement would help insure compliance with the ECPA disclosure requirements,[27] and would help prevent overbroad disclosures of blocked caller ID

[18] *Id.* at para. 23.

[19] *Id*.

[20] *Id.* at para. 29 (entities providing emergency services must be licensed by a state or municipality to provide such services to qualify for this exemption).

[21] AT&T Aug. 21, 2017 Comments at 4 ("To avoid creating any such conflicting obligations under Commission rules and the ECPA, the Commission should remove the proposed definition of 'threatening calls' and modify the proposed exception to Rule 64.1601(b) to be expressly consistent with Section 2702(c)(4) of the ECPA."); CTIA Aug. 21, 2017 Comments at 6 ("[t]he 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").

[22] AT&T Aug. 21, 2017 Comments at 2; CTIA Aug. 21, 2017 Comments at 9; Louis Taff Aug. 16, 2017 Comments at 2.

[23] AT&T Aug. 21, 2017 Comments at 1; CTIA Aug. 21, 2016 Comments at 5-6.

[24] 18 U.S.C. § 2702(c)(4).

[25] *Report and Order* at para. 14.

[26] *Id.* at para. 13.

[27] AT&T Aug. 21, 2017 Comments at 4-5 ("To avoid creating any such conflicting obligations under Commission rules and the ECPA, the Commission should remove the proposed definition of 'threatening calls' and modify the proposed exception to Rule 64.1601(b) to be expressly consistent with Section 2702(c)(4) of the ECPA. Specifically, the new exception to the Caller ID privacy rules should state that the privacy indicator for blocked (continued….)

information that may harm the privacy of non-threatening callers.[28] AT&T also states that a law enforcement safeguard would provide carriers with assurance that they are complying with the rules.[29] CTIA adds that requiring law enforcement involvement when restricted Caller ID information is requested would deter parties from manipulating the unblocking process.[30] Louis Taff believes a person with law enforcement experience should judge the circumstances surrounding a purportedly threatening call.[31] We find that, to ensure the exemption is not abused, a request for blocked Caller ID associated with a threatening call must be made by law enforcement on behalf of the threatened party.[32]

13. *No Liability For Carriers Under Our Blocked Caller ID Rules*. To the extent that AT&T asks the Commission to somehow exempt carriers from any other legal liability, we decline to do so.[33] Our concern is only with ensuring that Commission rules do not interfere with the ability of carriers to respond to law enforcement requests as allowed under law.[34] Carriers are not subject to liability for violating our Caller ID privacy rules if they disclose blocked Caller ID pursuant to our new exemption.[35]

14. *Spoofing*. AT&T suggests that the Commission undertake further efforts to thwart Caller ID "spoofing."[36] "Spoofing" occurs when a caller deliberately falsifies the information transmitted to the called party's Caller ID display to disguise their identity. Spoofing is often used as part of an attempt to trick the called party into giving away valuable personal information so that it can be used in fraudulent activity.[37] Federal law prohibits spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value.[38] Caller ID spoofing goes beyond the scope of this proceeding, but we are currently reviewing spoofing in other proceedings.[39]

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

15. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[40] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

(Continued from previous page)
Caller ID information does not apply where such information is the subject of a lawful request by a law enforcement agency as authorized by 18 U.S.C. § 2702(c)(4).").

[28] *See* AT&T Aug. 21, 2017 Comments at 4-6.

[29] AT&T Aug. 21, 2017 Comments at 5.

[30] CTIA Aug. 21, 2017 Comments at 7-10.

[31] *See* Louis Taff Aug. 16, 2017 Comments at 2.

[32] *Report and Order* at para. 16.

[33] AT&T Aug. 21, 2017 Comments at 6.

[34] *Report and Order* at para. 12.

[35] *Id.* at para. 12.

[36] AT&T Aug. 21, 2017 Comments at 6.

[37] *Report and Order* at n.21.

[38] 47 U.S.C. § 227(e)(1); *see also* 47 CFR § 64.1604(a); Federal Communications Commission, Spoofing and Caller ID, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id (last visited Sept. 19, 2017).

[39] In the Matter of Call Authentication Trust Anchor, Notice of Inquiry, Docket No. 17-97 (2017); *see also* AT&T Aug. 21, 2017 Comments at 6-7; Louis Taff Aug. 16, 2017 Comments at 2.

[40] 5 U.S.C. § 604 (a)(3).

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

16. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that will be affected by the proposed rules, if adopted.[41] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[42] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[43] Under the Small Business Act, a "small business concern" is one that: 1) is independently owned and operated; 2) is not dominant in its field of operation; and 3) meets any additional criteria established by the Small Business Administration (SBA).[44] Nationwide, there are a total of approximately 28.8 million small businesses, according to the SBA.[45]

1. Wireline Carriers

17. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[46] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[47] Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[48] Thus, under this size standard, the majority of firms in this industry can be considered small.

18. *Local Exchange Carriers* (*LECs*). Neither the Commission nor the SBA has developed a small business size standard specifically for local exchange services. The closest applicable size standard under SBA rules is for the category wired telecommunications carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and

---

[41] 5 U.S.C § 603(b)(3).

[42] 5 U.S.C. § 601(6).

[43] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 5 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[44] 15 U.S.C. § 632.

[45] SBA, Office of Advocacy, *Frequently Asked Questions*, https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf (last visited Sept. 19, 2017).

[46] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[47] *See* 13 CFR § 120.201, NAICS Code 517110.

[48] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[49] Under that size standard, such a business is small if it has 1,500 or fewer employees.[50] Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[51] Consequently, the Commission estimates that most providers of local exchange service are small businesses.

19. *Incumbent Local Exchange Carriers* (*Incumbent LECs*). Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable size standard under SBA rules is for the category wired telecommunications carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[52] Under that size standard, such a business is small if it has 1,500 or fewer employees.[53] Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[54] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses.

20. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate size standard under SBA rules is for the category wired telecommunications carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments

[49] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[50] 13 CFR § 121.201, NAICS code 517110.

[51] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[52] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[53] 13 CFR § 121.201, NAICS code 517110.

[54] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[55] Under that size standard, such a business is small if it has 1,500 or fewer employees.[56] Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[57] Consequently, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and other local service providers are small entities.

21. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (e.g., a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation."[58] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope.[59] We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

22. *Interexchange Carriers.* Neither the Commission nor the SBA has developed a small business size standard specifically for providers of interexchange services (IXCs). The appropriate size standard under SBA rules is for the category wired telecommunications carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[60] Under that size standard, such a business is small if it has 1,500 or fewer employees.[61] Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[62] Consequently, the Commission estimates that the majority of IXCs are small entities.

---

[55] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[56] 13 CFR § 121.201, NAICS code 517110.

[57] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[58] 5 U.S.C. § 601(3).

[59] Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, Federal Communications Commission (May 27, 1999). The Small Business Act contains a definition of "small business concern," which the RFA incorporates into its own definition of "small business." 15 U.S.C. § 632(a); 5 U.S.C. § 601(3). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. 13 CFR § 121.102(b).

[60] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[61] 13 CFR § 121.201, NAICS code 517110.

[62] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

23. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to other toll carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable size standard under SBA rules is for wired telecommunications carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[63] Under that size standard, such a business is small if it has 1,500 or fewer employees.[64] Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[65] Thus, under this category and the associated small business size standard, the majority of other toll carriers can be considered small.

2. Wireless Carriers

24. *Wireless Telecommunications Carriers (except Satellite).* Since 2007, the Census Bureau has placed wireless firms within this new, broad, economic census category.[66] Under the present and prior categories, the SBA has deemed a wireless business to be small if it has 1,500 or fewer employees.[67] For the category of wireless telecommunications carriers (except Satellite), Census data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms had fewer than 1,000 employees.[68] Thus under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) services.[69] Of this total, an estimated 261 have 1,500 or fewer employees.[70] Thus, using available data, we estimate that the majority of wireless telecommunications carriers can be considered small.

25. *Satellite Telecommunications Providers.* The category of satellite telecommunications "comprises establishments primarily engaged in providing telecommunications services to other

[63] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Categories"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[64] 13 CFR § 121.201, NAICS code 517110.

[65] 2012 U.S. Economic Census, NAICs Code 517110, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[66] U.S. Census Bureau, 2012 NAICS Definitions, "517210 Wireless Telecommunications Categories (Except Satellite)"; http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517210&search=2012%20NAICS%20Search.

[67] 13 CFR § 121.201, NAICS code 517210 (2012 NAICS). The now-superseded, pre-2007 CFR citations were 13 CFR § 121.201, NAICS codes 517211 and 517212 (referring to the 2002 NAICS).

[68] 2012 U.S. Economic Census, NAICs Code 517210, at http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[69] *Trends in Telephone Service*, tbl. 5.3.

[70] *Id.*

establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[71] This category has a small business size standard of $32.5 million or less in average annual receipts, under SBA rules.[72] For this category, Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[73] Of this total, 299 firms had annual receipts of under $25 million.[74] Consequently, we estimate that the majority of satellite telecommunications firms are small entities.

26. *All Other Telecommunications.* All other telecommunications comprise, *inter alia*, "establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry."[75] The SBA has developed a small business size standard for the category of All Other Telecommunications.[76] Under that size standard, such a business is small if it has $32.5 million in annual receipts.[77] For this category, Census Bureau data for 2012 show that there were a total of 1,442 firms that operated for the entire year.[78] Of this total, 1,400 had annual receipts below $25 million per year.[79] Consequently, we estimate that the majority of all other telecommunications firms are small entities.

3. Resellers

27. *Toll Resellers.* The Commission has not developed a definition for toll resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[80] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[81] Under that size standard, such a business is small if it has 1,500 or fewer employees.[82] Census data for 2012 show that 1,341 firms provided resale

[71] U.S. Census Bureau, 2012 NAICS Definitions, "517410 Satellite Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517410&search=2012.

[72] 13 CFR § 121.201, NAICS Code 517410.

[73] U.S. Census Bureau, 2012 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517410.

[74] *Id*.

[75] U.S. Census Bureau, 2012 NAICS Definitions, "517919 All Other Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2012.

[76] 13 CFR § 121.201, NAICS code 517919.

[77] *Id*.

[78] U.S. Census Bureau, 2012 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517919.

[79] *Id*.

[80] https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517911&search=2012+NAICS+Search&search=2012.

[81] 13 CFR § 121.201, NAICS code 517911.

[82] *Id*.

services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[83] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[84] Of this total, an estimated 857 have 1,500 or fewer employees.[85] Consequently, the Commission estimates that the majority of toll resellers are small entities.

28. *Local Resellers.* The SBA has developed a small business size standard for the category of telecommunications resellers. The telecommunications resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[86] Under that size standard, such a business is small if it has 1,500 or fewer employees.[87] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees.[88] Thus, under this category and the associated small business size standard, the majority of these prepaid calling card providers can be considered small entities.

29. *Prepaid Calling Card Providers.* The SBA has developed a small business size standard for the category of telecommunications resellers. The telecommunications resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[89] Under that size standard, such a business is small if it has 1,500 or fewer employees.[90] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees.[91] Thus, under this category and the associated small business size standard, the majority of these prepaid calling card providers can be considered small entities.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

30. This *Report and Order* creates an exemption for threatening calls and calls to non-public emergency services from our Caller ID privacy rules. These changes affect small and large companies equally, and apply equally to all classes of regulated entities identified above.

---

[83] 2012 U.S. Economic Census, NAICs Code 517911, at https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

[84] *Trends in Telephone Service*, at tbl. 5.3.

[85] *Id.*

[86] https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517911&search=2012+NAICS+Search&search=2012.

[87] 13 CFR § 121.201, NAICS code 517911.

[88] U.S. Census Bureau, 2012 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517911.

[89] https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517911&search=2012+NAICS+Search&search=2012.

[90] 13 CFR § 121.201, NAICS code 517911.

[91] U.S. Census Bureau, 2012 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517911.

31. *Reporting and Recordkeeping Requirements*. There are no new reporting requirements. This *Report and Order* amends the caller privacy rules to exempt threatening calls from the CPN privacy rules, so that associated law enforcement and, as directed by law enforcement, security personnel have quick access to information they need to aid their investigations. Voice service providers do not need to change their current recordkeeping as they have been able to provide CPN when requested in the past.[92]

32. This *Report and Order* adds a recordkeeping requirement. We amend our rules to allow non-public emergency services to obtain blocked Caller ID information associated with calls requesting assistance. Voice service providers will need to keep a record of when they provide blocked Caller ID associated with calls requesting assistance to non-public emergency services providers.

33. *Other Compliance Requirements*. Voice service providers will be required to release blocked Caller ID information when it is requested by law enforcement in conjunction with circumstances amounting to a threatening call and when a non-public emergency service requests blocked Caller ID. To do so, voice service providers must comply with law enforcement requests for CPN as they currently do under ECPA. We anticipate the impact will be small because of the statutory requirements already in place.[93]

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

34. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its approach, which may include the following four alternatives, among others: (1) the establishment of differing compliance or reporting requirements timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.

35. The Commission considered feedback from the *NPRM* in crafting the final order. We evaluated the comments in light of the goal of removing regulatory roadblocks to help security and law enforcement personnel responsible for the safety of parties receiving certain threatening calls obtain quick access to the Caller ID information needed to identify and thwart threatening callers. While a commenter suggested permissive rules, we implemented mandatory rules in light of public safety concerns.[94] We adopt an exemption instead of simply streamlining the waiver process to allow for virtually immediate access to blocked Caller ID information upon proper request in threatening situations.[95] The Commission considered continuing the waiver process, but inherent delays in the waiver process do not meet the goal of streamlining access to information needed to investigate threatening calls.[96] In addition, the Commission reduced uncertainty, burdens and costs on small business providers that seek to relay the

[92] *See, e.g.*, *INSIGHT 100 Petition for Waiver of § 64.1601(b) Regarding the Transmission of Calling Party Number*, CC Docket No. 91-281, Memorandum Opinion and Order, 17 FCC Rcd 223 (CCB 2002) (*INSIGHT Order*; *Rules and Policies Regarding Calling Number Identification Service – Caller ID; Petition of Chevrah Hatzalah Volunteer Ambulance Corps Inc. for Waiver of Section 1601(b) of the Commission's Rules – Blocked Telephone Numbers*, CC Docket No. 91-281, Order, 28 FCC Rcd 1253 (CGB 2013) (*Hatzalah Order*); *Petition of Liberty Public School District for Waiver of Federal Communications Commission Regulations at 47 CFR § 64.1601(b)*, CC Docket No. 91-281, Memorandum Opinion and Order, 28 FCC Rcd 6412 (CGB 2013) (*Liberty School Order*); *Middletown Order,* 31 FCC Rcd at 3565.

[93] *See* NTCA Sept. 19, 2017 Reply Comments at 2-3 (noting varying costs among small carriers in complying with existing law-enforcement requests under ECPA, but not discussing an expected increase in costs due to the proposed rules).

[94] *Id.* at para. 11.

[95] *Id.* at para. 10.

[96] *Id.*

blocked Caller ID information, by putting the identification of "security personnel" in the hands of law enforcement as opposed to providers.[97]

36. The Commission does not see a need to establish a special timetable for small entities to reach compliance with the modification to the rules. No small business has asked for a delay in implementing the rules. In considering the burden on small business, we note that they already have responsibilities under ECPA, and we align our threatening call definition with that of ECPA.[98] Similarly, there are no design standards or performance standards to consider in this rulemaking.

G. Report to Congress

37. The Commission will send a copy of the *Report and Order*, including this FRFA, in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act.[99] In addition, the Commission will send a copy of the *Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Report and Order* (or summaries thereof) will also be published in the Federal Register.[100]

[97] *Id.* at para. 18.

[98] *Id.* at para. 13.

[99] 5 U.S.C. § 801(a)(1)(A).

[100] *See id.* § 604(b).

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Rules and Policies Regarding Calling Number Identification Services – 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

The rash of threatening phone calls placed to many Jewish Community Centers earlier this year highlighted a disturbing trend: The number of threatening phone calls is on the rise.[1] This *Report and Order* responds to this development by enabling law enforcement to quickly obtain caller ID information following a threatening phone call to persons or property. This information could save lives and help apprehend those making such calls. Moreover, this measure is justified because callers who make threats should have no legitimate expectation of privacy that their caller ID information will remain secret.

I want to thank the staff for all their hard work on this *Report and Order*. From the Consumer and Governmental Affairs Bureau, thanks to Micah Caldwell, Nellie Foosaner, Karen Schroeder, Kurt Schroeder, Richard Smith, Nancy Stevenson, Mark Stone, Kristi Thornton, and Patrick Webre; from the Office of General Counsel, Douglas Klein, William Layton, Richard Mallen, Linda Oliver, and Bill Richardson; from the Wireline Competition Bureau, Kirk Burgee, Daniel Kahn, Melissa Kirkel, and Ann Stevens; and from the Office of Communication Business Opportunities, Belford Lawson.

[1] *See, e.g.*, Eric Levenson and AnneClaire Stapleton, Jewish Center Bomb Threats Top 100; Kids Pulled from Schools (Mar. 13, 2017), http://www.cnn.com/2017/02/28/us/bomb-threats-jewish-centers-jcc/ (reporting over 100 threats to 80 Jewish Community Centers); Associated Press, Statistics: Bomb Threats to Schools in New Hampshire are Up (Aug. 21, 2016), http://www.washingtontimes.com/news/2016/aug/21/statistics-bomb-threats-to-schools-in-new-hampshir/ (reporting an increase in threats to New Hampshire schools); United States Bomb Data Center, Bomb Threats across the U.S. (May 24, 2016), https://www.atf.gov/resource-center/docs/bomb-threats-across-us/download (finding an 84% increase in bomb threats to schools from 2010-2016 and an increase in bomb threats to residences) (ATF Report); Richard J. Bayne, Swatting Epidemic 'out of control' in Middletown School District (Feb. 27, 2016), http://www.recordonline.com/news/20160227/swatting-epidemic-out-of-control-in-middletown-school-district (reporting a rash of threats made to various schools in New York and the adverse impact on students); James Fisher, More School Threats in Region; FBI Assisting (Jan. 19, 2016), http://www.delawareonline.com/story/news/local/2016/01/19/fresh-round-school-threats-tuesday/78999668/ (reporting multiple phone threats to schools in Delaware, Virginia, Maryland, and Massachusetts).

STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN

Re: *Rules and Policies Regarding Calling Number Identification Services – 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

Sixty years ago, nine African American students made history when they entered the doors of Central High School in Little Rock, Arkansas. In the days following September 25, 1957, it was reported that threatening phone calls were received nightly in the homes of these history-making students.

What if Caller ID existed then and the identities of the perpetrators of these threatening phone calls were quickly shared with law enforcement personnel? Maybe, I choose to think through a current day lens that it would have made a difference. Unfortunately, even with advancements in technology, law enforcement personnel continue to face challenges with identifying and thwarting threatening telephone calls. This was evidenced earlier this year by the telephoned bomb threats made against Jewish Community Centers (JCCs) across this nation.

So today, the Commission acts on a bipartisan basis to ensure that when a threatening call is made, security and law enforcement personnel can quickly access blocked Caller ID information. By aligning our definition of a threatening call with the standard set in the Electronic Communications Privacy Act (ECPA), we enable a narrowly tailored exemption of our rules. Specifically, we establish that Caller ID information can only be provided to law enforcement when such a phone call "conveys an emergency involving danger of death or serious physical injury to any person requiring disclosure without delay of information relating to the emergency."

I am grateful for the work of the Consumer and Governmental Affairs Bureau for responding to the concerns initially raised by Senate Minority Leader Charles Schumer and following through with today's Order.

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *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

During this proceeding, I have endeavored to strike an appropriate balance between providing information to law enforcement to help them investigate threatening calls while safeguarding the valid privacy interests of callers who may choose to block caller ID to protect themselves or others from real harms. I also sought to narrow the circumstances under which loosely defined "security personnel" could obtain access to caller ID information. I wanted to ensure that providers are not put in an untenable role of deciding whether there is a threat and who should receive information. Additionally, we must protect call recipients from bad actors or others who may claim to be security personnel to get access to the information for their own purposes.

Given the Commission's penchant for TV references, let me delve into a couple to highlight that for every legitimate security personnel, there is a James Garner of the Rockford Files or Tom Selleck of Magnum P.I. seeking to extract information for unintended purposes. The item resolves this to a satisfactory degree, I hope, by tying security personnel to those approved or authorized by law enforcement.

I thank the Chairman and staff for working with me to resolve these concerns. I vote to approve.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *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

Over the past few years, we have seen a significant increase in bomb threats being called in to our schools, religious institutions, and community centers. According to one study, the number of bomb threats during the 2015-2016 school year more than doubled from three years earlier. And more than half of those threats were made by phone. In some cases, the perpetrators have been able to remain anonymous by taking advantage of an FCC rule that allows callers to block their caller ID information.

Today, we address this problem by adopting an exemption for threatening calls from our caller ID rules. Specifically, we allow carriers to disclose the blocked caller ID information associated with threatening calls to law enforcement, so that they can quickly identify and investigate the source of the threats. I am grateful that the FCC has moved quickly to address this issue, and the Order has my support.

Thank you to the Consumer and Governmental Affairs Bureau for their diligent work on this important item.