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

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

COMMENTS OF AT&T SERVICES, INC.

AT&T Services, Inc., on behalf of its affiliates, ("AT&T") submits these comments in response to the Notice of Proposed Rulemaking proposing to amend the Caller ID rules to facilitate the identification of threatening callers who block their Caller ID information.[1]

AT&T strongly supports the adoption of an additional exception to the Caller ID privacy rules to allow carriers to disclose the blocked Caller ID information of threatening callers, which otherwise may impede law enforcement investigations of threatening calls and hinder responses to these threats. To avoid subjecting carriers to potentially conflicting obligations, the Commission should structure this exception to be consistent with the requirements for carriers' disclosures of electronic communication record information established by the Electronic Communications Privacy Act ("ECPA"), which allows carriers to provide electronic communication record information to law enforcement only in specified emergency circumstances.

To help ensure the reliability of the information supporting these disclosure requests, as

[1] *Notice of Proposed Rulemaking*, FCC 17-76, CC Docket No. 91-281, rel. Jun. 22, 2017 ("Notice").

well as to help prevent the misuse of unblocking procedures to obtain the blocked Caller IDs of non-threatening callers, the Commission should require law enforcement to validate the existence of the circumstances supporting the disclosure of this information and should limit such disclosure to law enforcement.

AT&T also encourages the Commission to address the cheap and accessible Caller ID spoofing services that allow threatening callers to disguise their identities by spoofing the telephone numbers of innocent third parties.

I. THE COMMISSION SHOULD CLARIFY THE CALLER ID RULES TO ASSIST EMERGENCY LAW ENFORCEMENT REQUESTS

The Caller ID rules require carriers using Signaling System 7 to transmit the Calling Party Number ("CPN"), except where a caller dials *67 to request that the calling party number not be passed.[2] Terminating carriers are required to act in accordance with these privacy requests, except for calls made within limited systems, certain emergency calls, or calls subject to call tracing or trapping procedures requested by law enforcement.[3] In view of the increasing numbers of threatening calls, and the difficulties in addressing such calls that are created by the use of blocked Caller ID information to conceal the identities of threatening callers, the Commission proposes to adopt an additional exception in the Caller ID rules requiring carriers to provide threatened parties and law enforcement personnel with blocked Caller ID information for threatening calls.[4]

---

[2] *See*, 47 C.F.R. § 1601(a)-(b).

[3] *See*, 47 C.F.R. § 64.1601(d)(4)(i)-(iii).

[4] Notice, ¶¶ 2-3 & Appendix A, Draft Rule § 64.1601(d)(4)(iv). A "threatening call" would be defined as "any call that includes a threat of serious and imminent unlawful action posing a

(Footnote continued on next page)

1. Disclosure Should be Limited to Law Enforcement Requests Authorized Under 18 U.S.C. § 2702 (c)(4)

By seeking to expand the exceptions to the Caller ID privacy rules, the Commission properly recognizes the importance of ensuring that these rules do not hinder law enforcement in addressing threatening calls. To further this objective, however, the Commission's rules governing disclosures of blocked Caller ID information should be consistent with the requirements for the disclosure of electronic communication record information to government entities established by Section 2702(c)(4) of the ECPA.[5]

Section 2702(c)(4) of the ECPA allows a person or other entity providing an electronic communications service to the public to disclose information concerning a communication (not including the contents of a communication) to law enforcement (or other government entity) *only* "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 relating to the emergency."[6] However, the Notice would require carriers to provide blocked Caller ID information to law enforcement under much broader circumstances – "[u]pon report" of "any call that includes a threat of serious and imminent unlawful action posing a substantial risk to property, life, safety,

(Footnote continued from previous page)

substantial risk to property, life, safety, or health." *Id*., Appendix A, Draft Rules §§ 64.1600(l), 64.1601(d)(4)(iv).

[5] 18 U.S.C. § 2702(c)(4).

[6] *Id*. As described below, AT&T relies on law enforcement to validate the existence of emergency circumstances before disclosing information pursuant to Section 2702(c)(4) of the ECPA.

or health."[7]

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.[8] 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).

To avoid further conflict with the ECPA, the disclosure of blocked Caller ID information under any new exception to the Caller ID privacy rules should be voluntary, rather than mandatory as proposed by the Notice.[9] Under the ECPA, all permitted disclosures by carriers of stored wire and electronic communication record information that are not mandated by legal process, or required by a government entity pursuant to customer consent, are voluntary.[10]

2. The Circumstances Supporting Disclosure Should be Validated by Law Enforcement Rather Than by Carriers

The disclosure of blocked Caller ID information pursuant to any new exception to the Caller ID privacy rules should require confirmation by a law enforcement agency of the existence of the emergency circumstances as specified by 18 U.S.C. § 2702(c)(4) – that "an emergency

---

[7] Notice, Appendix A, Draft Rules §§ 64.1600(l), 64.1601(d)(4)(iv).

[8] *Cf.*, *Implementation of Section 309(J) of the Communications Act – Competitive Bidding*, 9 FCC Rcd. 4493 (1994) (amending the FCC competitive bidding rules to be consistent with other federal laws, policies and regulations).

[9] Notice, Appendix A, Draft Rule § 64.1601(d)(4)(iv) ("Upon report of such a threatening call, the carrier *will* provide any CPN of the calling party to the called party and/or law enforcement for the purpose of identifying the responsible party.") (emphasis added).

involving danger of death or serious physical injury to any person requires disclosure without delay of [blocked Caller ID] information relating to the emergency."[11] AT&T requires law enforcement to validate the existence of these required circumstances where disclosures of electronic communication record information are requested pursuant to Section 2702(c)(4) of the ECPA to help ensure the accuracy of the information supporting these requests. The Commission should similarly require law enforcement to validate the accuracy of the information supporting any requested disclosure of blocked Caller ID information. This safeguard would provide carriers with assurance that these disclosures comply with the ECPA, as well as help prevent overbroad disclosures of blocked Caller ID information that may harm the privacy of non-threatening callers.

Law enforcement personnel are indisputably better qualified to validate the existence of emergency circumstances than carrier personnel, and the Commission should allow carriers to rely on their expertise. Law enforcement personnel routinely make such evaluations in a wide variety of exigent situations and are likely to be more familiar with the facts giving rise to the requested disclosure.

Indeed, carriers would be subject to significant new burdens and costs if they were

---

(Footnote continued from previous page)

[10] *See*, 18 U.S.C. §§ 2702-2703.

[11] *See*, Notice, ¶ 13 (asking whether blocked Caller ID information should be provided only where law enforcement confirms the existence of circumstances meeting the Commission's proposed definition of a threatening call). As previously explained, the Commission should conform the circumstances under which its proposed exception would apply with those required under 18 U.S.C. § 2702(c)(4).

required to validate such facts as envisaged by the Notice.[12] To undertake such tasks, carriers may need to hire large numbers of personnel with law enforcement or similar experience, and/or conduct extensive training in the interpersonal communications and investigatory skills necessary to evaluate a caller's description and quickly determine whether or not there is a genuine emergency requiring the requested disclosure. Carrier personnel also would need to avoid being misled by those who inevitably would seek to exploit this potential opportunity to obtain restricted Caller ID information of non-threatening callers through misrepresentation in order to stalk a separated spouse or engage in other illicit activity.[13]

By requiring the existence of the required emergency circumstances to be determined by law enforcement, the Commission would reduce these potential risks. For the same reason, disclosures of restricted Caller ID information should be made only to law enforcement.

As a further safeguard for carriers, the Commission should provide that carriers would not be subject to any legal liability by providing blocked Caller ID information pursuant to the adopted rule.

II. THE COMMISSION SHOULD ADDRESS OTHER TECHNOLOGIES USED TO MAKE THREATENING CALLS

AT&T also encourages further efforts to identify individuals making threatening calls by spoofing the telephone numbers assigned to innocent third parties, including parties that utilize CPN blocking for lawful purposes. Regrettably, cheap and accessible technologies still foster the

[12] *See*, Notice, ¶ 13 & Appendix A, Draft Rule § 64.1601(d)(4)(iv).

[13] *See*, Notice, ¶ 15 (asking whether reports of threatening calls to obtain restricted Caller ID information should be made in conjunction with law enforcement "so as to provide some assurance that the called party is not attempting to circumvent the privacy obligations of the rule by reporting a false threat").

use of Caller ID spoofing as an instrument to defraud or otherwise harm called parties.[14] AT&T applauds the recent enforcement actions taken by the Commission against spoofed robocalling,[15] as well as the legislation recently passed by Congress to expand the FCC's enforcement tool kit to address violations of the Truth in Caller ID Act.[16]

To address the harmful effects of malicious Caller ID spoofing, the Commission also should give further consideration to imposing obligations on third-party Caller ID spoofing service providers.[17] The Commission has previously stated that it could revisit the issue once it had the opportunity to determine whether its current rules are sufficient to deter malicious Caller ID spoofing.[18] In light of the continuing nature of such harmful activities, the Commission should consider revisiting this issue, and whether it would be necessary to request any additional authority from Congress to undertake such action. For example, requirements that third-party Caller ID spoofing service providers maintain records of purchasers of their services and calls

---

[14] Robocall Strike Force Report, (Oct. 26, 2016) at 1. https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf ("Strike Force Report").

[15] *See*, *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, FCC 17-107, File No: EB-TCD-16-00023195, rel. Aug. 4, 2017 (Notice of Apparent Liability for Forfeiture); *Dialing Services, LLC*, FCC 17-97, File No: EB-TCD-12-00001812, rel. Jul. 26, 2017 (Notice of Apparent Liability for Forfeiture); *Adrian Abramovich, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc.*, FCC 17-80, File No: EB-TCD-15-00020488, rel. Jun. 22, 2017 (Notice of Apparent Liability for Forfeiture).

[16] 47 U.S.C. § 227(e). H.R. 423, the Anti-Spoofing Prevention Act of 2017, passed the House of Representatives on January 23, 2017, and a largely similar bill, S.134, the Spoofing Prevention Act of 2017, passed the Senate on August 3, 2017. *See also, Robocalls, a Problem we all Need to Solve*, AT&T Policy Blog (Jul. 6, 2016) https://www.attpublicpolicy.com/fcc/robocalls-a-problem-we-all-need-to-solve/.

[17] *See, Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, 26 FCC Rcd. 9114, ¶ 40 (2011).

[18] *Id.*, ¶ 41.

made using those services would assist investigations by law enforcement and the Commission of those who misuse these services.

The Commission also should encourage the efforts of current industry detection, assessment, trace-back, and mitigation efforts, which are specifically designed to facilitate the ability of law enforcement to quickly identify individuals making threatening calls.[19] The Commission should consider ways that it can facilitate such work, including by clarifying that carriers can share information to investigate and trace back unlawful calls to the source.[20] AT&T supports such collaborative efforts by the public and private sector to protect the public from these harmful activities, provided those efforts protect the legitimate privacy interests of calling and called parties.

Respectfully submitted,

By: /s/ James Talbot

James J. R. Talbot
Gary L. Phillips
David L. Lawson

Attorneys for
AT&T Services, Inc.
1120 20th Street, NW
Washington, D.C. 20036
(202) 457-3048

Dated: August 21, 2017

[19] *See*, Strike Force Report, *infra*, Sect. 3.

[20] *Id*., Sect. 4.2