Comments on Caller ID

CC Docket 91-281 - FCC Document 17-76

Louis Taff - taff@softwareestimatingprocesses.com

1. Introduction

I thank the FCC for the opportunity to comment on the NPRM and hope that my remarks are found useful. I agree with what I think is the intent of this NPRM, but wish to comment on some of its wording that, in my opinion, may restrict its scope such that it may not always accomplish its intended purpose. Additionally, I have comments on some privacy concerns of the FCC, threatened parties' rights and false claims.

2. Discussions

2.1 Definition of "Threatening Call"

Footnote 1 in Paragraph 1 states that for the purposes of this NPRM, the FCC proposes the definition of 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."

I am concerned about the words "serious", "imminent" and "substantial". These words each require someone to judge whether the threat is sufficient to justify initiation of law-enforcement action. My preference would be to eliminate these words and define a "'threatening call' as any call that includes a threat of unlawful action posing a risk to property, life, safety, or health."

I will try to explore scenarios that demonstrate how ambiguities in these words may have unfortunate consequences.

In Paragraph 3 we find the presumed justification for use of the word "imminent": the ability "to ensure that law enforcement personnel have quick access to the information they need to identify and thwart threatening callers, without the regulatory delay inherent in applying for and being granted a waiver of our rules."

Suppose that, for example, the content of a call were "A city council meeting will be blown up exactly one year from today." While I expect that everyone would say that the action posed by this threat is "serious," they would also conclude that the threat is not "imminent". Because the threat is not ***both*** serious ***and*** imminent, the call is not a threat for the purpose of this NPRM and would not be eligible for accessing its Caller ID. Presumably, law enforcement would find that the call ***is*** threatening by a less stringent definition, and would apply for a waiver of FCC rules to find out who made it.

If, however, the phrase "one year" in the above call were replaced by, say, "one week," one would have to debate whether or not it fit the NPRM's definition of a threatening call. Thus, my view is that precision of "imminent" will always be lacking, and may depend on the experience of local law enforcement, if any, in pursuing a waiver of FCC rules.

I could not find a definition of "serious" in the context of "serious action" in the NPRM, nor one of "substantial" in the context of "substantial risk". What criterion would the FCC promulgate to decide if a risk is "substantial"? A bombing in a crowded auditorium? The bombing of a single-occupant trailer? A threat to break someone's leg?

I think I would maintain that an advance warning of the possibility of ***any*** unlawful action by an individual or group that poses ***any*** risk to the property, life, safety, or health of another individual(s) or group(s) is a threat, given the condition that the action is unlawful. It seems to me that the decision to trace the perpetrator of a threatening call is best left to the law-enforcement agency to which the call is reported (see Paragraph 13).

My conclusion is that the terms "serious" and "substantial" in the definition of "threatening call", in addition to "imminent", lack precise meaning and are best omitted from the definition.

Let's consider the carrier employees who receive requests for Caller IDs. Today, these people presumably receive legal documents directing them to provide the Caller IDs. The employees need make no decisions at all, and simply execute the request and furnish the datum. Under the proposed rules, however, no one receives any paper. Someone from a law-enforcement agency will place a call to someone at the carrier, telling them that the call in question threatens an imminent crime that risks causing harm. What, now, is the carrier employee supposed to do? I fervently hope that the FCC is not implicitly authorizing this anonymous person without law-enforcement experience to judge the worthiness (i.e., its seriousness, imminence and substantialness of risk) of the threat and decide whether or not to provide the requested information without a formal waiver. If not, then the carrier must always take law-enforcement's word and immediately provide the Caller ID.

I expect that it would be a rare law-enforcement officer indeed who would initiate paperwork to get an FCC waiver rather than simply making a phone call to the carrier, even for a non-imminent threat. It seems to me, therefore, that the formal process of requesting a waiver of FCC rules will suffer an almost immediate death. Unless the FCC is prepared for this (and I hope it is), it must reconsider this NPRM.

2.2 The FCC's Privacy Concerns

Notwithstanding the NPRM's earnest discussion (Paragraphs 15-17) of the privacy rights of callers wishing to remain anonymous, the point is moot. The FCC knows, or certainly should know, that Section 64.1601(b) quoted by Paragraph 12 (p.5) is routinely violated by virtually every wireline carrier. Any wireline subscriber wishing to identify callers with blocked Caller IDs need only subscribe to an unblocking service such as Trapcall (www.trapcall.com) which claims some 850,000 customers. This capability was explicitly brought to the FCC's attention years ago by the Electronic Privacy Information Center in its comments on WC Docket 11-39. To my limited knowledge, despite its lip service to privacy, the FCC has yet to take any action on the issue.

The unblocking service exploits an industry-wide error in the specifications for the Call Forwarding feature. In Call Forwarding, when calls are forwarded, the Caller ID of the incoming call is used as the Caller ID of the forwarded call. This is usually what people want, e.g., to forward calls to their cell phones. Unfortunately, exactly the same procedure is used when forwarding calls to toll-free (i.e., 800) numbers. It should have been well-known to the writers and implementers of switching specifications that calls to toll-free numbers always deliver the Caller IDs, flagged for privacy or not, to the terminating customer. The justification has been that toll-free calls are paid for by terminating customers, who claim the right to know whose calls they are paying for. The error is that when calls are forwarded to toll-free numbers, no check is made by the forwarding entity (switch) to determine if the forwarded-to number is toll-free. A proper specification and implementation would make such a check, and if the privacy indicator is on, instead of the calling number, use the forwarding number as the Caller ID when forwarding to toll-free numbers. Callers who carefully block their Caller IDs (should) scrupulously avoid calling toll-free numbers, and have no way of knowing that a forwarded non-toll-free number ends up exposing their Caller ID.

On a personal note, I confess I myself was once quite concerned about the privacy implications of Caller ID transmission when Local Area Signaling Services first became available. When I expressed this concern to another individual, he was unexpectedly nonchalant about the issue. He noted that if transmission of Caller ID had been part of Alexander Bell's initial telephone invention, we would see it as simply part and parcel of the telephone, and not give it a second thought. I slowly came around to his view. The everyday analogy is to ask "Who's there?" before opening the door. If the FCC agrees with this idea, it can simply eliminate Caller ID blocking altogether.

2.3 Who Determines a Threat?

Responding to Paragraph 13, it seems to me to be circular logic to require that a threat be confirmed before a restricted CPN is released. Rather, I think the CPN should be released immediately, instantly, but only to law enforcement to verify the threat. I would leave it to the judgement of the law enforcement agency as to whether the threatened party should receive the number. This would help mitigate the risk of releasing the CPN on a false claim.

The last sentence of Paragraph 13 suggests that to save time, threatened parties could be granted access to the Caller ID without involving law enforcement. It is easy to conclude that if law enforcement need not be involved, there is no incentive for call recipients to restrict their Caller ID requests to threatening calls. For better or worse, this will end Caller ID blocking.

2.4 Threatened Parties' Rights

I feel that threatened parties have a right to know who made the call, but only if law enforcement determines that the threat was real or a hoax rather than a legitimate caller. Hence, as above, this can be satisfied by having law enforcement, not the carrier, reveal the caller to the threatened party.

2.5 False Claims of Threats

Paragraph 15 raises the issue of possible false reports of threats. In my mind, this danger is mitigated by two factors. First, filing such a false police report is illegal, and presumably carries criminal penalties; it is advisable that the police warn complainers of threatening calls of this fact when taking their reports. Second, if my suggestion above to release the CPN only to the authorities is followed, the false claim may not allow the claimant access to the CPN in any case.

3. Appendix A – Draft Proposed Rules for Public Comment

I propose the following edit of Appendix A to reflect my comments.

1. Amend § 64.1600 by changing paragraph (1) to read:
(l) *Threatening Call*. The term "threatening call" means any call that includes a threat of unlawful action posing a risk to property, life, safety, or health.

§ 64.1601 Delivery requirements and privacy restrictions.

(iv) Is made in connection with a threatening call. Upon report by law enforcement of such a threatening call, the carrier will provide any CPN of the calling party to law enforcement for the purpose of identifying the responsible party.