Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

To: The Commission

COMMENTS OF
THE BOULDER REGIONAL EMERGENCY TELEPHONE SERVICE AUTHORITY

The Boulder Emergency Telephone Service Authority ("BRETSA"),[1] by its attorney, hereby submits its Comments on the Commission's June 7, 2019 Third Further Notice of Proposed Rulemaking ("FNPRM") in the above-captioned matter. BRETSA's Comments address only protection for Critical Calls discussed at Section IV.B., paragraphs 63-70 of the NPRM.

I. Emergency Notification Service Calls Are Robocalls.

Emergency Notification Service ("ENS") involves autodialing all landline telephones located within a defined geographic area, and all wireless (portable or nomadic phones) registered to addresses within the defined geographic area; and delivering a prepared or pre-recorded message. Many ENS providers maintain geographically distributed facilities from which ENS calls can be placed.[2] ENS calls may also present a caller-number and caller ID associated with agency which initiates the calls. ENS calls are thus robocalls, are intended to be

[1] BRETSA is a Colorado 9-1-1 Authority which establishes, collects and distributes the Colorado Emergency Telephone Surcharge to fund 9-1-1 Service in Boulder County, Colorado.
[2] ENS call center locations are selected so that the call centers are not likely to be simultaneously affected by conditions which interfere in their operation, or by the same incidents which prompt use of the ENS service.

transmitted from different locations than that of the agency causing the ENS calls to be transmitted, may provide caller numbers and caller IDs of the agency causing the ENS calls to be transmitted rather than of the ENS provider, and may appear the same as the marketing and fraudulent robocalls which the Commission seeks to prevent.

Recent advances in WEA have improved the service and made it available for use by local jurisdictions, so that it may supplant ENS in some cases. However residents of mountainous areas such as those in Boulder County continue to subscribe to traditional wireline service, due to the unavailability of ubiquitous and reliable wireless services in mountainous areas due to terrain shielding for example.[3]

The Commission must assure that ENS calls are not blocked along with the marketing and fraudulent robocalls it intends be blocked.

II. 9-1-1 Calls Made Using Traditional And New Communications Services Must Not Be Blocked.

In its Declaratory Ruling, FNPRM para. 34, the Commission "clarify[ies] that voice service providers may offer opt-out call-blocking programs based on any *reasonable* analytics designed to identify unwanted calls." BRETSA maintains that analytics designed to identify unwanted calls are *not* reasonable if they identify 9-1-1 calls as unwanted calls.

BRETSA understands that new calling services and service configurations are being developed, sometimes integrating diverse devices or technologies. These new services and service configurations, and service innovation in general, will serve the public interest. However it is possible that new or currently available innovative services would trigger call-blocking

[3] While wireless text-messaging coverage exceeds wireless voice coverage; BRETSA understands that text-coverage advantage will decrease significantly as wireless providers replace SMS text-messaging with session-based RTT and *emulated* SMS text-messaging.

based on analytics developed for extant or more broadly-used calling technologies, services and configurations.

BRETSA has stated that new personal communications services should be required to include a 9-1-1 solution prior to authorization to avoid the situation where cellular service was available for almost a decade before providers were even required to accept 9-1-1 calls and connect them to *a* PSAP. Similarly, there should be a means to review both call-blocking analytics and systems, and existing and new *bona fide*[4] telephony services, service configurations or solutions, to verify that (i) call-blocking solutions are based on *reasonable* analytics, (ii) calls including 9-1-1 calls placed using new *bona fide* telephony services, service configurations or solutions are not blocked by extant call-blocking solutions, (iii) the Commission has the opportunity to require modification of call-blocking solutions to accommodate new *bona fide* telephony services, service configurations and solutions, and (iv) the Commission has the opportunity to determine that a new telephony service, service configuration or solution would unreasonably undermine the ability of service providers to block robocalls, and to determine that analytics which would result in blocking calls made over such new service, configuration or solution are nevertheless reasonable. BRETSA believes the Commission should establish a voluntary test-bed for this purpose.

Absent such a test-bed, providers and users of new telephony solutions may find calls unexpectedly blocked, including 9-1-1 calls. In the case of 9-1-1 calls, Emergency Response may be delayed or prevented (and claims for damages and findings of liability may result). In other

[4] While BRETSA does not wish to inhibit development and introduction of new and innovative telephony and telecommunications services, configurations and solutions; it is clear that large profits can be reaped from robocalling for marketing purposes or in support of efforts to defraud consumers. BRETSA would not want any such means of testing robocall blocking solutions and whether they block 9-1-1 calls made over extant and new services or service configurations to provide a testing ground for robocall providers or users to identify means of defeating robocall blocking solutions or caller ID authentication solutions.

words, it would be better to determine if calls may be blocked in advance so that remedial action can be taken before marketing and deployment of a solution, rather than after a call such as a 9-1-1 call has been blocked.

BRETSA believes that voluntary participation by service providers and developers of new telephony services, service configurations an solutions in a testing program administered by the Commission, through its Office of Engineering and Technology for example, would (i) provide for representations of voluntary participants to be made under penalty of perjury as a deterrence to misuse of the test-bed, (ii) allow the Commission to verify that voluntary participants are *bona fide* developers or providers of telecommunications services and not robocall providers seeking means to defeat robocall-blocking solutions, (iii) allow protection of intellectual property rights of participants, and (iv) establish that voluntary participants have acted prudently to avoid inadvertent blocking of calls, as a defense to claims under state law for damages resulting from any inadvertent blocking of calls which does occur.

III. Outbound Numbers Of PSAPs and Government Emergency Outbound Numbers.

With respect to protections for critical calls, the Commission proposes to maintain a "Critical Calls List" that providers may not block which "would include at least the outbound numbers of 911 call centers (*i.e.*, PSAPs) and government emergency outbound numbers—numbers that we believe all consumers would not want blocked." FNPRM, para 63. Unlike ENS robocalls transmitted from an ENS provider's data center, BRETSA does not understand why a call made from a PSAP or government agency would appear to reasonable analytics as a robocall. However there have been instances in which BRETSA representatives have received spam robocalls identified as coming from a BRETSA-affiliated city government (and even robocalls to the representative's cellphone shown as coming from the representative's own

wireline phone number with their own name in the caller ID, received while the representative was seated within feet of the wireline handset which remained on-hook).

It is clear that robocallers will spoof government numbers, and BRETSA presumes they would spoof outbound PSAP, Office of Emergency Management or other public safety agency numbers and caller IDs, so that the call would appear to be coming from a trusted authority. Entering these numbers on a Critical Call List could thus make it easier for robocallers to spoof these numbers and make it appear their calls are coming from a trusted authority, making called parties more vulnerable to attempts to defraud them.

It is critically important that outgoing calls from governmental entities including public safety agencies *not* be blocked. BRETSA has previously placed the transcript and link to the recording of a 9-1-1 call and related calls in the records of Commission proceedings. In that case, a 9-1-1 call was received from a man reporting that a friend had called him threatening to commit suicide by stepping in front of a semi. After gathering the information from the caller, the dispatcher called the suicidal man's wireless provider to request it ping the location of the suicidal man's device. The provider waived the requirement that the dispatcher fill out a paper form requesting the ping and fax it to the provider, due to the urgency of the situation.[5] Upon

[5] In 2019, with all of the technical advances implemented by service providers and PSAPs; when lives are at stake and seconds count, PSAPs must still (i) identify the carrier from which a suicidal individual or other person whose location they need to ping takes service, and (ii) fill out a paper form, and fax it to the carrier to request the carrier ping the individual's device's location (although this requirement is waived by wireless providers in some cases. BRETSA continues to believe that service providers should establish a secure web portal for a single clearing house to which PSAPs could electronically submit a user numbers for determination of which carrier supplies service, and request the user device to which the number is assigned be pinged for its location. The clearing house should then either forward the user number to the appropriate carrier for automatic location determination, or the clearing house itself should determine and return the device location to the PSAP if the service provider supplies the clearing house with access to its systems to determine subscriber device locations. In the case described above, the suicidal man stepped in front of the semi during the eight minutes that the dispatcher was on hold with the carrier waiting for the location information to be provided (and the carrier had waived the requirement that the PSAP fill out and fax the form to the carrier before undertaking to determine the device location in that case). Reducing the amount of time required to ping locations of user devices, for instance in the context of the surprising number of 9-1-1 calls placed by or concerning suicidal individuals, would save lives.

being provided the device location by the wireless provider, the dispatcher called the PSAP serving the jurisdiction in which the caller's phone was located. After being advised by that second PSAP that a 9-1-1 call had just been received of a man stepping in front of a semi in the area in which the suicidal man's phone was located, the dispatcher called the man who had made the original 9-1-1 call advising him that he would be contacted by an investigator and when the man asked, confirming that the suicidal man had followed through on his threat.

Just from this example, it would appear that by spoofing a PSAP number and caller ID for a fax or voice line, (i) an unauthorized party could obtain an individual's device's current location from a wireless provider, (ii) a person could call a different PSAP and provide information about fictitious incidents to tie-up First Responder units or for some other illicit purpose, and (iii) appear to the general public to be a person with respected authority.

The Commission should identify as an aggravating factor in any rule violation pertaining to robocalls, and request Congress pass legislation identifying as an aggravating factor in any statutory violation, the spoofing of telephone numbers of governmental entities including public safety agencies (except in the case of ENS calls placed on behalf of a public safety agency), authorizing assessment of additional penalties or award of additional or exemplary damages in any civil action based upon a violation of the applicable rules or statute. Because it is more expensive and difficult to assess and collect administrative forfeitures, criminal fines or civil judgments against foreign actors, reducing the efficacy of deterrence of foreign actors; any reasonable means of identifying and blocking robocalls which originate in foreign countries, and calls which originate in foreign countries with spoofed caller IDs, should be implemented. Robocalls originating in the U.S. prompting people in the U.S. to call foreign numbers which

may appear to be domestic numbers,[6] or which connect completed calls to parties in foreign countries, cannot likely be automatically blocked because the offensive character of those calls is based upon the content or actions taken after a domestic call is connected. However these calls do originate as domestic calls subject to deterrence, and BRETSA believes the offensive character of these calls should constitute aggravating factors warranting increased penalties in a regulatory or criminal context or exemplary or punitive damages in a civil context.

IV. Protection of Emergency Service Numbers.

In the early days of autodialers, instances were reported in which autodialers placing marketing or nonprofit donation solicitation calls would serially dial numbers, including Emergency Service Numbers ("ESNs") associated with 9-1-1 trunks, and tying up all 9-1-1 lines in PSAPs. While it is not clear to BRETSA that this issue, or an IP-based variant of this issue, will be of concern in an NG9-1-1 ESInet environment such as will soon be implemented in Colorado; legacy E9-1-1 service in Colorado will be phased out over the next two years and may continue to be provided in other states for a longer period.

Because outgoing PSAP calls are not placed over PSAP inbound 9-1-1 trunks, these numbers should not be included on any Critical Call lists identifying sensitive numbers which should *not* be blocked. Inclusion of ESNs on any Critical Call Lists, if accessible by the public or individuals with malicious motives, could enable parties to conduct total denial of service-*like* attacks by tying up 9-1-1 trunks used to deliver 9-1-1 calls to legacy PSAPs. The same concern would arise if these numbers have been published to avoid autodialers being programmed to dial these numbers serially, and tie up PSAP 9-1-1 lines. However it would appear the same result could be accomplished by mandating autodialers dial numbers randomly. Randomly dialed

[6] See FNPRM, para. 14.

robocalls including marketing calls would still be received by PSAPs, but serial dialing of ESNs, simultaneously blocking all 9-1-1 lines into a PSAP, would be avoided. Alternatively, including ESNs in lists of numbers which may not be included in robocall/autodialer call lists, without identifying them as ESNs and without distinguishing them from consumers opting out of such call lists, may also protect against parties intentionally tying up all 9-1-1 lines into a PSAP.

Respectfully submitted,

BOULDER REGIONAL EMERGENCY TELEPHONE SERVICE AUTHORITY

By: 

Joseph P. Benkert

Joseph P. Benkert, P.C.
8506 Porcupine Pointe
Parker, CO 80134
(303) 948-2200

Its Attorney

July 24, 2019