

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

Rules and Regulations Implementing the
Telephone Consumer Protection Act of 1991

Establishing Just and Reasonable Rates for
Local Exchange Carriers

CG Docket No. 02-278

WC Docket No. 07-135

Comments of Robert Biggerstaff

Robert Biggerstaff submits these comments on the letter from the National Association of Attorneys General regarding technology approaches to protecting consumers from illegal robocalls.¹

Many of the proposals for blocking robocalls operate by taking some action *after* the call has reached the user's phone. While the responsive action can be nearly instantly implemented (such as silencing the ringer) a common flaw in these systems is that the call has to hit the handset *first*, and thus impose a cost on both the consumer and on the shared resources of the wireless infrastructure. Many cell phone users will still have to pay to "receive" those robocalls and robotexts.

While I heartily encourage exploration of technology to "block" illegal robocalls after they are made, I believe what is desperately needed, is a way to choke off the source where these calls are *entering* the national telecommunications' infrastructure. Instead of swatting mosquitoes, drain the swamp.

¹ Letter from Indiana Attorney General Greg Zoeller et al. to Tom Wheeler, Chairman, Federal Communications Commission (Sept. 9, 2014); *Public Notice*, DA 14-1700 (Nov. 24, 2014).

Preventing illegal robocalls from entering the network also avoids many of the issues raised by inter-carrier blocking. Even if inter-carrier blocking was implemented, its success depends in large part on accurate metadata *about* the calls in order to provide that metadata to the end user or to use that data in categorizing—and potentially dropping—the call if the consumer opted-in to such an action.

Issues related to “false positives” in blocking technology would also be mooted by preventing illegal robocalls and robotexts from entering the network.

Analogies to Spam E-mail.

Robocalls and robotexts have much in common with spam e-mail. Spam e-mail sometimes makes up over 90% of e-mail message volume in the world. If the technological initiatives currently in place (such as the realtime blacklist or “RBL”) were not in place, e-mail worldwide would be unusable. The nature of e-mail and SMTP routing makes such technical measures feasible. Importantly, the address of the computer where the spam enters the Internet e-mail system can always be determined and responsive action taken.² Those measures can isolate spam e-mail at its source so it never reaches its destination. This is what is needed for robocalls and robotexts and it requires one simple thing—that the source of every robocall and robotext entering the network can always be determined by any IXC or LEC in the path, and particularly by the terminating carrier.

² Indeed, such measures were so successful at countering “bulletproof” spam hosting providers, that e-mail spammers had to adapt. Most now rely on hijacking individual users’ PCs to send out spam from their home computers. Such an adaptation by robocallers would be practically impossible with wireline networks, since it would require much more sophisticated hacking of much more hardened targets than a random person’s personal computer.

No one should be able to inject untraceable³ calls into the network. No one. Failure of a carrier to be able to ID the source of a call it carries should be considered a serious failure of its responsibilities to protect the public welfare.

Others on this docket have echoed the value of a source identification approach to address robocalls:

[R]egulators and AGs should be looking for solutions that can track calls to their source(s) and stop them. End-user complaints pour into the FTC and other repositories at the rate of thousands per day. We (meaning the industry, regulators and technologists) should be using that complaint data in combination with carrier signaling records to automatically trace calls back, even with spoofed or randomized Caller-ID. Once the source (or "ingress point") is identified, illegal mass-calling campaigns can be quickly shut down.⁴

I believe a critical first step is to implement technological initiatives in order to reliably identify the point source of the "emissions" of illegal robocalls. You can't even begin to implement blocking (or prosecutions) unless you can identify the source. The better (faster, more accurate, more difficult to defeat) the identification is, the better the resulting actions (such as blocking or routing to voice mail) can be.

Many illegal robocalls and robotexts (from now on, I'll use "calls" to mean calls and text messages) originate at "boutique" phone carriers that exist solely to serve such scofflaw users rather than to serve legitimate businesses. This is akin to web hosting companies that provide "bullet proof" hosting to spammers. They often intentionally keep little or no records of calls, and even fewer records of their clients. Instead they allow

³ I do not mean "blocked" callerID. CallerID blocking unfortunately has some minor legitimate uses. I am talking about **untraceable** calls that cannot be traced by the carriers, which evade call logs maintained by carriers, and for which a carrier cannot even identify the source when served with a court order or subpoena.

⁴ *Comments of ZipDX LLC*, at 2, dated Jan 22, 2015,

clients to remain anonymous behind foreign mail drops. Anyone who tries to find the source of these calls will find many lead back to shadowy, virtually untraceable companies such as Transfers Argentina, Asia Pacific Telecom, TeleEurope, and Castle Rock Capital Management.⁵

As just one example, one investigation into Jamie Dunn and the company Voice Touch, revealed⁶ startling details that are unfortunately all too common in the robocalling industry:

In his second conversation with Zykan,⁷ Dunne directs Zykan to [the] following website address: WWW.telcl.info. Dunne then provides temporary login credentials to Zykan and walks him through a demonstration of how Voice Touch clients use this website to manage their robocalling campaigns. At the conclusion of this demonstration, Dunne states: "Yeah, we mask the [ANI]. We mask the [ANI] so that nobody can - they mask the [ANI] so that they can never trace who the call is coming from." Upon information and belief, in this quoted passage, Dunne is using the acronym ANI, which stands for "Automatic Number Identification." ANI is a service that tells the recipient of a telephone call the telephone number of the person initiating the call.

In his second conversation with Zykan, Dunne claims that he has made over one billion "dials" for Voice Touch client National Auto Warranty Services, Inc. ("NAWS").

In their second conversation, Dunne assures Zykan that he would be "bulletproof" because Zykan would not be contracting with Voice Touch, but with an "offshore company" named "International Business Corp. where we're listed as an anonymous beneficiary." Dunne further claims that he has "trustees that are in Hong Kong" as well as "protectors, which would be like maybe the Central Bank of Belize." Finally, Dunne states that there is "another layer" which he describes as "Panamanian foundations set up now

⁵ Through what can only be described as Herculean efforts, the FTC was able to unwind the Byzantine system of shell companies to identify the principles behind some of these entities. This is obviously beyond the resources of the average consumer.

⁶ *Declaration of Roberto C. Menjivar* at ¶¶18-20, (Doc. 42 in *FTC v. Network Foundations, LLC.*, No. 1:09-cv-02929 (N.D. Ill. 2009)).

⁷ Zykan identifies himself to Dunne as the president of a prospective Voice Touch client.

so that the money goes from the IBC [International Business Corp.] ... over to a Panamanian foundation which goes out to Bank Swiss." In conclusion, Dunne states, "it's impossible to track, impossible for them to find out who the company is."

This is what consumers are up against.⁸

For spam e-mail, this "bulletproof" hosting issue dealt with by the RBL—"if you don't convince your customer who is spamming to stop, then we will not accept *any* e-mail from your server." I believe there should be a way that the same principle can apply to telephone carriers. It is complicated by the fact that phone companies have special obligations to customers not necessarily present in the context of providing e-mail service. But there are a number of measures that can be taken to address misuse without actually denying service. If the existing regulations do not permit a carrier to drop traffic from a scofflaw who permits his clients to spew forth thousands of robocalls an hour, then those regulations need to be changed to expressly permit such action to protect the network from such abuse.

Step 1: Traceability of all calls to their source.

The first and most important measure is to ensure that the source of calls and texts can *always* be identified.⁹ This step must be implemented regardless of what additional technological approaches to robocalls are contemplated. This is the single most important step in combating illegal robocalls and robotexts. Unless and until this is accomplished, there will always be ways for the scofflaws to remain "bulletproof."

⁸ See also *id* at ¶30 totaling the amount paid to Voice Touch by just one robocalling client (National Auto Warranty) during a 10 month period at \$6,013,500.

⁹ Even if the source cannot (currently) be identified *in real time*, there is no excuse for a carrier to be unable to identify the source of a call when requested later, such as through an investigative demand or subpoena.

My work as a computer forensic examiner and dealing with hundreds of subpoena responses from phone companies has revealed that there are gaps in phone company records, particularly in the ability to identify the source of some calls. These gaps rarely appear to affect records of calls from friend, family, or legitimate businesses. But those gaps plague phone carrier records of illegal robocalls. I frequently see carriers claim in subpoena responses that there are no phone records available that identify the source of calls I and others clearly received since there are recordings of the calls as they were received and the terminating switch logged the call. These data I have reviewed strongly suggest that illegal robocallers have exploited capabilities to not only falsify callerID, but to mask or alter out-of-band identifiers (such as ANI) that traditionally could not be altered by the caller. This raises three questions for me. If such calls are untraceable, I wonder if terrorists are as smart as telemarketers. The second, is whether the Department of Homeland Security would tolerate a phone company not being able to trace a call back to its source. The third, is why does the Commission tolerate this? The Commission should review the applicable technical standards and make changes to harden the national telecommunications infrastructure against such attacks on call metadata.

Stopping spoofed callerID is next. The effect of the introduction of callerID on “prank” phone calls is instructive. Widespread introduction of callerID led to a rapid and significant decline in those calls due to the perception of callers that they could be easily identified. Prank calls, such as “swatting” have made a resurgence due in large part to technologies that permit the source of calls to be masked.

It is necessary to actually *stop* falsified callerID, not merely pass a rule prohibiting it. One of the most useless changes to the TCPA was the provision to weakly prohibit falsified

callerID. There is no practical way to prove it for most people,¹⁰ much less prosecute it. Like many criminals, robocallers never expect to get caught. Their robocalls are already illegal. Tacking on false callerID both helps them evade blocking mechanisms and evade being identified. They simply believe they are “bulletproof” to TCPA prosecutions. Unfortunately, they are often correct.

While implementing technological changes to prevent callerID spoofing, there are steps that can be taken now to at least flag callerID that is spoofed, similar to how an e-mail program may flag suspected spam e-mail without actually blocking it.

There are simple changes that can be incorporated in the callerID standards that would permit consumers (and carriers) to know when a call has falsified callerID. Some of these can even be implemented in a way that is backwards compatible with existing callerID technology so wireline users can benefit from those changes as well as wireless users. These can involve something as simple as doing additional database lookups and indicating the results (such as with a flag that callerID or ANI is false on the callerID display) or as complex as a complete overhaul of ANI and callerID. Carriers can integrate data from Service and Equipment Indicator (SEI), Originating Line Number Screening (OLNS), Billing Name and Address (BNA), and even Service Start Date (SSD) to develop a score for a call in the same way spam e-mail blocking software scores incoming e-mail.

¹⁰ I am aware of only one case where a consumer successfully prosecuted a case for false callerID, and that consumer had to go to the expense of purchasing expensive callerID hardware that recorded and printed the callerID payload, as well as verifying and recording the accuracy of the checksum. That consumer also had to retain an expert witness to provide the foundation for the admissibility and interpretation of the callerID logs and the accuracy of the hardware reporting it. This is obviously beyond the resources of the average consumer.

Obviously, a common tactic used by illegal callers is manipulation of callerID. But some customer-service call centers have a legitimate need to manipulate callerID so it shows a callback number that will receive inbound calls for their client rather than a number that rings to the call center. A solution would be to require a carrier who wants to permit a customer to manipulate their outbound callerID, to require a significant bond from each such customer and positive identification, similar to the “know your customer” program that is currently used to prevent money laundering in financial services. Legitimate companies that want to manipulate callerID will have no problem obtaining a bond and providing identification and references. Scofflaws, on the other hand, will balk.

Carriers serving such customers (who want to alter their callerID) should also be required to maintain additional logs of calls, to facilitate investigatory efforts if complaints lead back to such a customer, and enforce appropriate terms of service. Such carriers should be required to verify that any outgoing manipulated callerID is in fact a phone number the calling party has registered with the carrier as legitimately used by the caller. The same rules should apply to callerID manipulation services, such as “SpoofCard”¹¹ as well as callerID “rental” services such as Telephone Management Caller ID, LLC., which profit on CNAM dips. The same should apply to VOIP POPs.

Carriers with no caller-ID spoofing customers will have no burden at all. If a carrier chooses to allow a customer to manipulate their callerID, that customer can—and should—foot the bill for whatever resources the carrier needs to accommodate them.

Also, carriers are charging consumers for enhanced callerID (i.e. CNAM delivery) but not doing CNAM lookups outside their own databases. For example some do not dip LIDB

¹¹ <http://www.spoofcard.com/>

(e.g., for CNAM) on every call, but instead deliver a generic UNAVAILABLE/OUT OF AREA or just a location (NPA-NXX) derived string. e.g., “MASSACHUSETTS” or “LEXINGTON MA.” This needs to stop. Consumers who pay for CNAM lookups should get CNAME lookups on every call. Wireless carriers need to start delivering CNAM on every call also.

Step 2 - Action

The second critical step is to increase the likelihood that illegal callers will be *caught*. That is accomplished with a two-pronged strategy of *detection* and *rapid response*.

Law enforcement has been very successful using volunteers “in the field” to form the first line of defense against illegal callers. For example, the FBI used retired citizens affiliated with AARP—and equipped them with tape recorders to gather evidence on illegal callers targeting the elderly. Known as “Operation Senior Sentinel,” this operation was immensely successful in taking a bite out of the illegal calls targeting the elderly. The Commission, along with the FTC, should consider a similar operation to address robocalls and robotexts. Once again, the analogy to spam is useful, and in this case, spam “honeypots” have proved a very useful tool.

The old adage of “follow the money” applies to illegal robocallers. The volunteers should be given traceable credit cards to use that are set up to capture any inquiry against the card. When the volunteer gives “Rachael at Card Services” the traced credit card number and a charge is attempted or the card’s balance/validity is checked, a CID should *immediately* go out to the clearinghouse that processed the charge to identify their client.

Hand-in-hand with detection, there needs to be a swift-footed response to that detection. When an illegal robocall is detected and the recording forwarded to the investigative unit, a CID should go out *immediately* to the carrier(s) involved. The

Enforcement Bureau should be turning these around in hours after a complaint is filed, not weeks or months.

The Commission should consider its experience with the dial-a-porn problems in the past, which were addressed by application of existing Commission guidance where some boutique carriers were responsible for a disproportionately large number of violations. Application of existing standards such as “a high degree of involvement or actual notice of an illegal use and failure to take steps to prevent such transmissions”¹² is also called for to address some of these “wink and a nod” relationships between carriers and robocall platforms, and between robocall platforms and their clients.

Act now

The time to explore these options is now, particularly with an eye to the sunset anticipated for the PSTN, and to ensure the packet-switched networks that replace the PSTN are bulletproof against scammers and illegal robocallers.

CONCLUSION

Blocking illegal robocalls one at a time with technology is a worthy goal. Stopping them from entering the network in the first place would be orders of magnitude better and more effective. But for both strategies, effective identification of the calls depends on improvements in call metadata record-keeping and reliability.

¹² See, e.g., Citation letters from Kurt A. Schroeder, Deputy Chief, FCC Telecommunications Consumers Division to Kevin Katz, Fax.com President (Dec. 26, 2000; May 11, 2001; May 31, 2001) (citing *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, *Memorandum Opinion and Order*, 10 FCC Rcd 12391, 12407 (1995) (*TCPA Memorandum Opinion and Order*)); *TCPA Report and Order*, 7 FCC Rcd 8752, 8780 (1992) (quoting *Use of Common Carriers*, 2 FCC Rcd 2819, 2820 (1987)).

At some point fewer and fewer points of entry will be available to illegal robocallers and the time period in which they can operate before they are shut down will become so short that robocallers will conclude that it isn't worth it.

Respectfully submitted, this the 23th day of January, 2015.

/s/ Robert Biggerstaff