BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	GC Docket No. 17-59
Advanced Methods to Target and Eliminate	)	
Unlawful Robocalls	)	
	)	DA 18-638
	)	

COMMENTS OF NOBLE SYSTEMS CORPORATION

Filed July 20, 2018

Karl Koster
Chief Intellectual and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

Contents

I. Introduction

Noble Systems is a global provider of contact center software and hosted contact center services serving customers in a variety of industries and applications, both domestically and internationally. Noble Systems submits these comments in response to the Public Notice[1] issued by the Federal Communications Commission ("Commission") seeking comment on the progress made by industry, government, and consumers in combatting illegal robocalls, and the remaining challenges. Noble Systems encourages the Commission to: (i) align the Commission's terminology (namely "robocalls") with that used by other federal agencies to reduce confusion, (ii) encourage carrier deployment of unambiguous per-call blocking signaling indications and industry development of call blocking/labeling mitigation mechanisms to ensure legal communications are not unduly impacted, (iii) continue focusing on the development of SHAKEN/STIR as the framework for a long term solution to the problem of illegal calls.

II. An Opportunity to Align Terminology

It is not surprising that the volume of illegal calls continues to increase. One web site tracking "robocalls" alleges that in June of 2018, over 4.1 billion such calls were made in the U.S.[2] Regardless of how these calls are identified, the number has been increasing over time. Other carriers have reportedly introduced technology to block over a billion unwanted automated calls last year, but yet the volume still increases.[3] In addition, FTC reports a year-over-year increase in robocalls.[4]

While the exact number of "robocalls" measured by some of these sources may not be precise, there is a discrepancy between how the Commission and other entities define what constitutes a "robocall." It is difficult to measure, discuss, and resolve the "robocall" problem when there is no consensus as to what a "robocall" is. On this point, the Commission's definition

[1] Public Notice: Consumer and Governmental Affairs Bureau Seeks Input for Report on Robocalling, FCC, CG Docket No. 17-59, DA 18-493 (June 20, 2018).
[2] Robocall Index, YouMail, https://robocallindex.com (last accessed July 9, 2018).
[3] http://about.att.com/sites/cybersecurity/ni/robocall (accessed July 16, 2018).
[4] See, e.g., https://www.ftc.gov/news-events/press-releases/2017/12/ftc-releases-fy-2017-national-do-not-call-registry-data-book-dnc, accessed July 19, 2018.

is out-of-step with industry definitions and other government agencies. The FTC defines a robocall as when "you answer the phone and hear a recorded message instead of a live person, it's a robocall."[5] Merriam-Webster defines a robocall as "a telephone call from an automated source that delivers a prerecorded message to a large number of people."[6] Some law firms consider a robocall as a "pre-recorded telemarketing message."[7] Finally, some states also consider a robocall to be calls "with prerecorded telemarketing messages."[8] Granted, there is not consensus that the pre-recorded message must be a telemarketing message, but there is a common understanding that a robocall involves a pre-recorded message of some form.

The Commission in the past has defined "robocalls" as including calls playing a pre-recorded announcement as well as calls made using an automated telephone dialing systems ("ATDS") to one of the restricted numbers or destinations.[9] There has been great debate and uncertainty as to what constitutes an ATDS. Under the Commission's definition, a call made where an agent is connected to a wireless number is not a robocall if the agent manually dialed the number, but the call may be a robocall if some other technology were used. Similarly, a call made using an ATDS to an administrative (non-emergency) telephone number to a police station may not be a robocall, but if made using an ATDS to an emergency number at the police station, then it is a robocall. Finally, a call to an office in a hospital may not be a robocall if made using an ATDS, but if directed to a guest room in the hospital then it may be a robocall.

Significant uncertainty exists with the Commission's current definition of a robocall as to what is, or is not, a robocall. In contrast, there is little ambiguity as to when a call plays a prerecorded message. Many callers can easily and clearly identify in the first few seconds after answering a call when a prerecorded message is played. As the Commission is revisiting its definition of an ATDS in a separate rulemaking, the Commission can use this opportunity to finally align its definition of a "robocall" with that of other government agencies. Namely, the Commission should align the definition of a "robocall" with the FTC, so that a common understanding is achieved of this term. This will facilitate comparison of robocall call volume

[5] https://www.consumer.ftc.gov/features/feature-0025-robocalls, accessed 7/17/18.
[6] https://www.merriam-webster.com/dictionary/robocall.
[7] http://robocalllaw.com/.
[8] http://consumer.georgia.gov/consumer-topics/robocalls.
[9] That is, calls made without consent to e.g., an emergency line, hospital, doctor's office, health care facility, guest or patient room of a hospital or elderly home, as well as to a number assigned to a cellular service.

data and robocall solutions. The Commission can separately address ATDS originated calls from robocalls, and avoid further confusion. This point has been reiterated in the past by other commentators. As used herein in these comments, the term "robocall" is used to mean calls that play a prerecorded announcement to the called party.

It is apparent that the growth in robocalls has not been impeded by the existing statutes and regulations. Nor does it appear that broadening the scope of the definition of an ATDS in Commission's regulations has reduced the number of illegal robocalls. For example, the Commission recently fined one individual for $120 million for making millions of illegal calls.[10] The decision by that individual to make the calls was likely motivated because the caller could easily evade identification by spoofing unauthorized numbers. Further, many callers originate their calls outside the U.S. where jurisdictional and technical issues make their identification and prosecution even more difficult.

One universal characteristic of these illegal call originators is that they rely on anonymity in making their calls by spoofing unauthorized telephone numbers. VoIP technology has made it incredibly easy for scammers to hide by using a false calling party number ("CPN"). Further, some will spoof a reputable company's telephone number in order to increase answer rates. In fact, some scams (like the so-called "IRS scam") attempted to take advantage of the government's reputation. Using a spoofed CPN makes it sufficiently difficult that only the largest and most egregious scammers warrant the allocation of regulatory or law enforcement resources to trace and identify them. Thus, it should be recognized that the fundamental issue to be addressed with illegal robocalls is determining when a call originator is spoofing an unauthorized number to avoid identification. The issue is complicated because there are many legitimate and useful applications of spoofing, and the practice of spoofing an authorized CPN must be distinguished from using an unauthorized CPN.

III. Call Blocking and Labeling Are Useful But Limited Solutions

One way industry has responded to the problem of illegal robocalls is by developing various mobile applications and carrier services that can block or label incoming calls. Consumers

[10] Forfeiture Order, *In the Matter of Adrian Abramovich, et al.*, File No.: EB-TCD-15-00020488, FCC 18-58 (May 10, 2018).

can choose from hundreds of mobile applications and many of the major carriers offer one or more call labeling/blocking services. These products and services are proving to be useful tools in the consumer's arsenal to combat unwanted or illegal calls.

However, these solutions frequently use analytics to predict the type of call by using a proprietary algorithm analyzing (in part) the CPN. However, it is acknowledged that this process is not 100% perfect. Nevertheless, it provides some relief from many illegal or unwanted calls. The issue is that legitimate and wanted calls can be erroneously "tagged" by these algorithms, with the result that legitimate or wanted calls are treated as scam or fraudulent calls. Anecdotal evidence suggests that legitimate call originators have encountered a 15-25% reduction in connection rates due to these services.

A. Issues Remain With Call Blocking/Labeling Technology

When a call is blocked, service providers blocking the call may provide a busy signal back to the calling party. Doing so provides misleading information to the calling party, as the caller is unaware that their call has been blocked. Thus, this has been sometimes called a "fake" busy signal. Contact center operators frequently program their dialers to reattempt a call to a number at a later time when encountering a busy condition, causing additional calls. Providing a unique signaling cause code or audio intercept message to the call originator would inform the caller that the call was blocked. The caller would likely cease further attempts and decide whether to investigate further. At least the caller is not deceived and can decide how to address the situation. At that point the caller may use various mitigation procedures provided by the service carrier to address alleged incorrect handling of the call.

Providing a fake busy signal is misleading, and does not accurately inform the caller of the status of the call. Industry participant have been lamenting that one impact of robocalls and spoofing is that the public no longer "trusts" the telephone network, to the point that they no longer answer call. The calling party number cannot be trusted. Allowing service providers to provide a fake busy indication when blocking calls is further eroding the public's trust in the telephone network. The Commission is the guardian of the telephone network and should address this issue. Just as the Commission is addressing illegal spoofing, it should address carriers providing fake

busy signals. Allowing carriers to provide a fake busy signal appears to violate the letter, if not the spirit of the Commission's rulings.[11]

Noble Systems, along with other industry participants, have suggested that service providers could provide an explicit, unambiguous indication that the call was blocked. Providing an audio intercept (similar to those audio announcements informing the caller that the called number is not in service) is within the capability of every service provider. This capability could be used to inform the caller that the call has been blocked, and the intercept message could inform the caller how to access the carrier's mitigation procedures, e.g., by verbally indicating a URL or telephone number.

Allows erroneous call blocking to continue can cause harm to both the called party and the calling party. Since the called party will not receive the call, they will not know if they have missed a wanted call. The caller, upon being informed that the call was blocked, could at least investigate whether a mistake occurred. Thus, instances where a mistake has occurred, such as the erroneous blocking an automated prescription refill reminder call, can at least be identified for further investigation. Otherwise, calling parties will simply reattempt the call, only to be blocked again.

B. Need for Mitigation Procedures

Noble Systems, along with PACE[12], and other industry participants, have been working to develop call blocking/labeling mitigation procedures through a PACE sponsored forum called the Communication Protection Coalition ("CPC"). The purpose of the CPC forum is ensure that mitigation procedures are defined for those instances when calls are erroneously blocked or mislabeled. The CPC is premised on recognizing that occasional mistakes will be made when

[11] *See, e.g.*, Declaratory Ruling, *In the Matter of Developing a Unified Intercarrier Compensation Regime; Establishing Just and Reasonable Rates for Local Exchange Carriers*, CC Docket No. 01-92, WC Docket No. 07-135, DA 12-154 (Feb. 6, 2012) at ¶ 13 ("The Commission has found that practices by common carriers that deceive or mislead customers are unjust and unreasonable practices under section 201(b). It is a deceptive or misleading practice, and therefore unjust and unreasonable under section 201(b), to inform a caller that a number is not reachable or is out of service when the number is, in fact, reachable and in service.") ("2012 Ruling").
[12] Professional Association for Customer Engagement.

service providers block or label calls. But, there must be a way for determining when a mistake has been made and then a way to mitigate the mistake. This requires:

1) Informing the caller that the call has been blocked (so the caller knows a potential mistake has occurred),
2) Identifying the carrier serving that called party number (so the caller knows which carrier to contact), and
3) Identify a channel used by that carrier to process an inquiry or a request to mitigate the treatment of calls using the calling party number (so the caller knows how to make the request).

Informing the call originator that the call is blocked can be done with the aforementioned per-call blocking indication provided via a signaling cause code and/or intercept announcement. The identification of the carrier serving the called party number can be readily ascertained using various publically available resources. However, in regard to the third step, many carriers have yet to identify a URL, telephone number, or other contact for receiving mitigation requests. There are no standards yet defined for how this information is to be provided, nor a timeframe for when a response should be provided to an inquiry. For many call originators, which may use hundreds of different CPNs and periodically alter the CPN for different calling campaigns, attempting to manually inquire on a per-number basis and wait several business days for a response to an inquiry is simply unworkable. The Commission should continue to monitor such industry activities, and should consider initiating a Notice of Proposed Rulemaking on this particular topic.

The need for mitigation procedures for call blocking not only applies to the current analytics based call blocking/labeling, but will also applies when SHAKEN/STIR is deployed. It is envisioned that unattested calls in SHAKEN/STIR may be blocked by a terminating service provider, and it is quite possible that technical issues may arise causing a call to be incorrectly classified as unattested. If so, the caller should know that the call was blocked, should be able to investigate why the call was blocked, and should be able to mitigate the error. Thus, even in a SHAKEN/STIR environment, there is the need for a per-call blocking indication required to be conveyed to the calling party along with offering mitigation procedures. Returning a fake busy signal in this situation does not help. It would be inappropriate for the Commission to encourage

the industry expending their resources to rebuild trust back into calling party number by deploying SHAKEN/STIR only to erode that trust by allowing the use of fake busy signals.

The Commission should consider various mechanisms to ensure timely development of a per-call blocking indication and adequate mitigation capabilities that can also be applied to SHAKEN/STIR. One such mechanism is requiring carriers to implement the per-call blocking indication along with mitigation capabilities before any safe-harbor can be granted to a service provider when they incorrectly block/label a call. This will provide motivation for the service provider to deploy these capabilities.

It is recognized that mobile smartphone applications and carrier services may accomplish similar end results, but in different ways. For example, mobile applications may label calls or may suppress ringing on the mobile device upon receipt of the call, resulting in a similar user experience as carrier-based call blocking or labeling. However, developers or users of mobile applications are not subject to the Commission's carrier regulations and this difference means regulatory obligations or incentives to carriers may not be applicable to mobile application providers/users. The fact that there are different regulatory requirements for carriers than for mobile application developers/users should not be the basis for avoiding obligations on the carriers in this matter. Thus, arguments that because a mobile application does not have to return a per-call blocking indication when ringing is suppressed to the mobile subscriber should not be a reason to relieve carriers from returning a per-call blocking indication to the caller.[13]

IV. SHAKEN/STIR is the Long Term Solution

The root cause of so many illegal and unwanted calls is because the caller is, in effect, anonymous. Scammers originating illegal calls use VoIP, because they can easily spoof an unauthorized telephone number. Pranksters who call E911 call centers to dispatch police to a residence (a practice call "swatting") always spoof their number; without spoofing, the practice would not exist. Threatening callers (such those making bomb threats) rely on spoofing to hide their true number.

[13] Nevertheless, there are industry proposal allowing users to indicate this from their device to the carrier. See, e.g., https://tools.ietf.org/html/rfc8197, accessed July 19, 2018.

The industry has been working towards deploying SHAKEN/STIR as a solution to this problem. While it is possible to still make illegal or unwanted calls with SHAKEN/STIR, these callers can be identified easier, cheaper, and faster. We can expect at some point during the proliferation of SHAKEN/STIR technology that unattested calls will be regularly blocked or routed to voicemail. Carriers have announced that deployment of SHAKEN/STIR will begin starting in 2019.[14] Based on past comments to the Commission, there appears consensus that this solution should be encouraged by the Commission. It is important, however, that the SHAKEN/STIR technology allows contact center operators to legitimately spoof calls (i.e., number they are authorized to spoof), as there are many useful and legitimate applications for spoofing.

V. The Commission Should Not Be Distracted from the Long Term Solution

The problem with unwanted and illegal call origination largely stems from callers spoofing unauthorized numbers. This problem will not be solved by "tinkering" with the definition of an ATDS or increasing penalties of the TCPA. As experience has shown, scammers ignore the TCPA, the DNC, and Truth-in-Caller ID statutes and other regulations because they can remain anonymous by spoofing. While call blocking and labeling are useful technologies, and represent one tool for reducing illegal or unwanted calls, that technology is inherently limited as it does not identify a particular call as spoofing an unauthorized calling party telephone number.

Industry has observed how scammers have evaded call blocking/labeling techniques by altering their spoofing tactics. Scammers were using a single spoofed telephone number for all their scam calls and observed their calls were being blocked or not answered. As expected, scammers have migrated to "neighbor spoofing" which is harder for algorithms to discern from legitimate calls using related numbers. Call blocking/labeling is analogous to the carnival game of "whack-a-mole" where scammers migrate to the next technique until algorithms catch up. Neighbor spoofing is difficult to stop, but if neighbor spoofing is effectively addressed, then

[14] See, e.g., https://transnexus.com/blog/2018/verizon-outlines-their-plans-to-stop-robocalls-using-shaken, accessed July 19, 2018.

scammers may start using public service telephone numbers. Without SHAKEN/STIR, some very hard decisions will need to be made at that point as to how this problem will be addressed.

The Commission should not lose focus on the long term solution that involves deploying SHAKEN/STIR. While call labeling/blocking has some short term advantages, it should not detract from deploying SHAKEN/STIR as a long term solution. Even after SHAKEN/STIR is deployed, there is still a role for providing a per-call blocking indication and mitigation procedures. Thus, ensuring development of a per-call blocking signaling indication and mitigation procedures is applicable to the long term solution as well.

VI. Conclusion

In light of the Commission's activities of re-interpreting the scope of an ATDS in the TCPA, the Commission has an opportunity to align their definition of a "robocall" with that of other government agencies and industry. Doing so will reduce confusion as to the types of calls being addressed and facilitate discussion of the solutions.

The cause of the problem will illegal robocalls, i.e., those calls which play a pre-recorded announcement to the called party, is largely a result of callers being able to easily spoof unauthorized numbers. Spoofing allows the call originator to remain anonymous. While analytics based call blocking and labeling does partially address the problem of robocalls, that technology can also erroneously block or label wanted and legitimate calls. It cannot readily distinguish between legitimate an illegitimate spoofing. The long term solution is to deploy SHAKEN/STIR technology.

Respectfully submitted on July 20, 2018,

/Karl Koster/
Karl Koster,
Chief IP and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338
(404) 851-1331 (x1397)