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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
	)	
To: The Commission	)	

REPLY COMMENTS OF ZipDX

David Frankel
dfrankel@zipdx.com
17554 Via Sereno
Monte Sereno, CA 95030
Tel: 800-372-6535

Filed: July 24, 2017

Contents

I. The Record Shows No Quantitative Support for Proceeding With the Four Blocking Components of the NPRM

Any proposed regulation should have clear benefits that outweigh the costs it imposes. The benefits envisioned by the NPRM would be a reduction in illegal robocalls and fewer scams perpetrated on vulnerable call recipients. The costs include industry expense to implement the actions envisioned by the proposed regulation, the costs to administer the proposals, the potential blocking of legitimate calls, both domestic and international, and the consequential damages arising from the inability of parties to make and receive those legitimate blocked calls.

The NPRM itself offers no quantitative assessment of any of these factors, yet it is clear that there are significant costs associated with the proposals and minimal consumer benefits.

All four elements of the NPRM will impose significant implementation costs including technical and administrative costs, They are easily evaded by robocallers. They provide no discernable immediate or longer-term benefits.

At (8), the NPRM formalizes Do-Not-Originate by permitting "voice service providers [to] block calls using a spoofed Caller ID number if the number's subscriber requests that they do so."[1]

The Strike Force suggested a desire to "block calls where the Caller ID shows an unassigned number"[2] and the NPRM codifies this at (16): "We can readily identify three categories of unassigned numbers. Those categories are: 1) numbers that are invalid under the North American Numbering Plan (NANP), including numbers with unassigned area codes; 2) numbers that have

[1] NPRM FCC 17-59, para, 8

[2] Robocall Strike Force Report, October 26 2016, at page 40. https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf

not been allocated by the North American Numbering Plan Administrator (NANPA) or the National Number Pool Administrator (PA) to any provider; and 3) numbers that the NANPA or PA has allocated to a provider, but are not currently assigned to a subscriber. In this NPRM, we seek comment on rules to codify that providers may block numbers that fall into each of these three categories."[3]

The NPRM states at (17): "[B]ecause these numbers are not valid, there is no possibility that a subscriber legitimately could be originating calls from such numbers. Nor do we foresee any reasonable possibility that a caller would spoof such a number for any legitimate, lawful purpose; for example, unlike a business spoofing Caller ID on outgoing calls to show its main call-back number, invalid numbers cannot be called back. We therefore do not see a significant risk to network reliability in allowing providers to block this category of calls."[4]

Unfortunately, this benign "risk assessment" is contradicted by observed network traffic. It cannot be and is not supported by comments in favor of the NPRM that simply reproduce content from the Notice without offering any additional insight.[5] It is disappointing that the Strike Force, whose membership includes twenty carriers, apparently did not review their own

[3] NPRM, para. 16

[4] NPRM, para. 17

[5] In the Comments of 30 State Attorneys General (AG Comments), the group states: "There is little risk in allowing providers to block calls from the following: (1) an assigned number when the number's subscriber requests calls from that number to be blocked, (2) invalid numbers, (3) numbers not allocated to a provider, and (4) numbers that are allocated to a provider but not assigned to a subscriber." https://ecfsapi.fcc.gov/file/10706088301496/State%20AG%20Comment%20on%20FCC%20Proposed%20Robocall%20Rule.pdf, page 3. T-Mobile offers this: "T-Mobile also agrees that the Commission should allow carriers to block calls from invalid numbers and from valid but unallocated numbers. Permitting carriers to take these steps will allow T-Mobile to preemptively reject many fraudulent calls, and will free its customers of the requirement to proactively request blocking of those calls. As the Commission notes, there is no possibility that incoming calls from invalid and unallocated phone numbers could be legitimate calls, and blocking such calls bears no risk to network reliability." https://ecfsapi.fcc.gov/file/10703249378046/T-Mobile%20Comments%20on%20Robocall%20NPRM%20(7-3-17).pdf, page 3

data on the billions of actual telephone calls passing through their networks daily prior to making the suggestion that they be permitted to implement the suggested blocking. Even in responding to the NPRM, none have come forward with any call data from their records. Had they looked, the carriers would have found that there are entire categories of legitimate, desirable traffic that would be ensnared by the NPRM's proposed "unassigned numbers" filters. We cover this more fully in our assessment below.

II. Cost-Benefit Analysis of Do-Not-Originate

A. DNO Benefits are Negligible

One perceived benefit of the DNO filter is to reduce the prevalence of robocall scammers impersonating, for example, IRS enforcement officials. The Attorneys General state: "These scammers often spoofed legitimate IRS numbers, which helped trick many consumers into giving scammers thousands or even tens of thousands of dollars. By stopping this type of spoofing, the FCC can cut down on the efficacy of such scams, likely saving consumers across the country millions of dollars."[6] While some have given a DNO trial credit for a reduction in complaints about the IRS robocall scam, we and others have identified a different reality. USTelecom states in their comments: "As demonstrated by last year's enforcement action targeting illegal robocall call centers in India, the arrest of the criminals originating those calls dramatically reduced consumer impacts."[7] The credit for any sustainable decrease in IRS scam calls goes to the police in India, not DNO.

[6] AG Comments at page 2.

[7] Comments of The USTelecom Association at page 6, available at https://ecfsapi.fcc.gov/file/10703149098952/USTelecom-Blocking-Comments-2016-07-03-FINAL.pdf

B. Working Around DNO is Easy

Even if DNO had any effect in this situation, DNO is easily evaded by robocallers; once his favorite number is on the DNO list, the robocaller will move to another. Further, common sense tells us that the vast majority of the American public does not know and would not recognize the IRS's toll-free number. If a vulnerable recipient of one of these calls were to be at all suspicious, what is most likely is that they would call back the number from which they purportedly received the call, and ask if they are really in trouble. If a valid IRS number is being spoofed, the IRS would likely serve taxpayers better if they did NOT block that spoofing of their number(s), and instead had operators standing by to explain the situation to would-be victims until we fix the problem another way.

A further described benefit of DNO is that the IRS (in this example) doesn't want their number(s) spoofed, and DNO would allow them to prevent that as long as the IRS and/or others acting on its behalf don't use the number(s) to place outbound calls. But DNO would just drive robocallers to use some other number(s) and now whatever burden accrued to the IRS for the use of THEIR number would fall on the owner of the new number. According to the Strike Force, "bad actors could easily and rapidly transition to randomized and/or legitimate telephone numbers in order to circumvent DNO blocks… [with] the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify."[8]

DNO is easily overcome by techniques in wide current use by robocallers, and it will be entirely ineffective.

[8] Industry Robocall Strike Force Report, April 28 2017, page 25, available at https://ecfsapi.fcc.gov/file/10428413802365/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf

C. Costs and Risks of DNO are High

The are no benefits to the implementation of DNO, yet DNO is costly. In the Strike Force 2017 report, the group writes:

> As happened during one of the trials, legitimate calls will be blocked if any carrier attempts to implement blocks of purported inbound-only numbers without fully vetting the subscriber's understanding that the number is inbound-only. Such false positives should of course be avoided in the first instances, and if they do occur they need to be remedied promptly. In the near term, any widely deployed efforts would likely face significant technical scalability issues, in addition to the policy risks (e.g. incentivizing more spoofing of legitimate numbers in order to get around DNO blocks) discussed above. For example, the network capabilities for all providers operating in today's voice ecosystem varies widely. In some instances, an individual carrier may even have disparate network capabilities within their respective networks (e.g., portions of the network may be TDM, while other portions may be IP-based). As a result, as any centralized list of DNO numbers grows, it may very well exceed the capacity of certain network systems. In addition, there is currently no centralized method for obtaining blocking authorizations across the universe of network providers. As a result, letters of authority (LOAs) from each number's owner must ideally be sent to each organization seeking to institute a DNO blocking process, since there is currently no form of 'transitive' authorization. In order to implement DNO blocking process on a broader scale, some form of universal LOA would need to be developed. In addition, some form of centralized distribution method for such LOAs would need to be developed, along with a list management framework. Regarding this latter point, any such list would need to be continually monitored and updated as telephone numbers are added to, or removed from, the list of authorized DNOs, while keeping such information out of nefarious hands."[9]

USTelecom states: "[B]ecause of the nature of DNO – outright blocking of calls in the network – *it is crucial that a heightened level of due diligence and ongoing maintenance by voice providers is resident throughout the entire process*."[10] (emphasis added) They continue: "[I]t is crucial that DNOs implemented by industry are tracked and coordinated through a central effort. Absent such coordination, the subscriber could end up in a situation where they lose track of which carriers are instituting DNOs. In a scenario where the subscriber wishes to remove the

[9] Strike Force April 2017, page 26

[10] USTelecom, page 8

DNO (e.g., the number(s) will start making outbound calls, or is reassigned), it will be imperative for all carriers instituting the DNO to be aware of the need to remove the block(s). *Only through a centralized and coordinated effort can such efficiencies and network integrity be obtained.*"[11] (emphasis added) And they state: "*Ongoing maintenance of the telephone number prior to and during the DNO must also take place* in order to ensure that the disposition of the telephone number at issue does not change over time. Among other things, such scenarios can arise if the DNO telephone number is changed to permit outbound calls, or if it is reassigned to another entity. Any such change may trigger a requirement that the number is removed from its DNO status."[12] Neustar recognizes these requirements and states in their Comments: "*Establishing a system to maintain this information could be costly, and it is not clear that such a system could be implemented without the risk that legitimate calls will be blocked in error*." [13] (emphasis added)

Thus, implementation of a robust, reliable, scalable DNO capability is problematic and expensive – a huge price to pay for something with no discernable short- or long-term benefit.

Alternatives are available, and not expensive: In their Comments, Neustar presents a far, far less costly alternative to DNO that still addresses at least some concerns about a fraud call containing an inbound-only calling party number: "[A] modified DNO solution can still work by informing the subscriber through the Caller Name display that the call is 'Fraudulent.' Any consented-to DNO numbers can be loaded in recognized industry CNAM databases to provide

[11] USTelecom, page 9
[12] USTelecom, footnote 16
[13] Comments of Neustar, Inc. at page 6, available at https://ecfsapi.fcc.gov/file/10703221599506/Neustar%20Robocalling%20Comments.pdf

the 'Fraudulent' display to protect consumers when their provider is not able to support DNO call blocking."[14]

Along similar lines, the April 2017 Strike Force report references Verizon's use of existing CNAM infrastructure warning the called party of a "potential spam call."[15]

Modifying the CNAM databases at the request of the subscriber to the number is a trivial process already supported by existing network infrastructure and processes.

DNO as proposed in the NPRM should be abandoned and CNAM solutions should be promoted. This approach requires no Commission rulemaking.

III. Cost-Benefit Analysis of Blocking Calls Originating from Unassigned Numbers

A. Benefits of Blocking Unassigned Numbers are Minimal

In our filed Comments, we presented a quantified analysis of the FTC robocall complaint database showing that the fraction of complaints related to calls from "unassigned numbers" was miniscule. We did not see any other comments that attempted to quantify the benefits of these filters.

Sprint states: "The first category of calls identified by the Commission—invalid numbers—does lend itself to relatively easy processes to block such calls. But *Sprint's experience does not show this category to be a large problem at this time.* Anecdotal reports suggest that most recent robocalls originate from a spoofed number that is local to the recipient. … [B]locking additional categories of numbers, such as unassigned blocks or individual

[14] Ibid, page 6

[15] April 2017 Strike Force report, page 17.

unassigned numbers, is less likely to be effective as the robocalling spoofers will choose to use randomly selected numbers, which may or may not be allocated for use. Therefore to apply blocking 'on all unused numbers' would likely result in little gain to the consumer. More likely at this point the robocallers would resort to the use of spoofing legitimate names and numbers, thereby bypassing industry's efforts to block unassigned and invalid numbers."[16]

Thus, we conclude that this set of blocks would have no measurable, sustainable benefit.

B. Costs and Risks of Blocking Unassigned Numbers are Unacceptably High

The costs, on the other hand, loom quite large. Many commenters expanded on the Commission's concerns raised in the NPRM regarding "Calls Originating From Numbers That Are Allocated to a Provider, But Not Assigned to a Subscriber."[17]

There is no list or database of such numbers and no apparent practical, cost-effective way to build one. That is not the largest problem; the most troubling aspect of the "Unassigned Numbers" proposal is the huge number of legitimate calls that would be improperly flagged as "invalid" and blocked, and the tremendous (unacceptable) cost associated with such massive improper call blocking.

In its comments, USTelecom writes: "USTelecom maintains that voice providers should still exercise caution in instituting such call blocking. For example, while numbers that do not reflect the traditional 10-digit structure of those assigned by the NANP could presumably be targeted for such blocking, *legitimate calls from foreign numbers can potentially be blocked since many*

[16] Comments of Sprint Corporation at pages 5-6. Available at https://ecfsapi.fcc.gov/file/10630203670739/Sprint%20Robocalling%20Comments.pdf
[17] NPRM, paragraphs 22 and 23.

do not follow the NANP format. … [T]here can be instances of legitimate domestic calls reflecting seemingly 'invalid' numbers."[18] (emphasis added)

USTelecom made no mention of the *magnitude* of this risk, but we know it to be huge. This failure is rooted in the technical details of how calls are processed in the PSTN and in particular how the "Caller-ID" is generated and propagated. We know that participants in this proceeding are reluctant to wade into technical details, but such details are core to how radically this part of the NPRM fails in real life and must be addressed.

Given how important technology and network realities are to this aspect of the NPRM, it is concerning that none of the carrier participants in this docket, or their representatives, presented any technical analysis in their Comments.

The fundamental issue is that there are MANY reasons that legitimate calls might present an "invalid" Caller-ID, and there is no reliable way to discriminate between these situations, and those where a robocaller has spoofed an invalid ID.

We have attached an Appendix A, which presents the relevant technical details and explains them. Commenters and the Commission ignore these details at their peril. We hope they will share this Appendix with their technical colleagues to get a substantive and trusted perspective on the details presented.

Briefly, in lay terms, the problematic scenarios FOR LEGITIMATE CALLS include:

- Calls from a business PBX which is not properly configured and sends as Caller-ID something invalid, such as just the last four digits of the caller's extension.

[18] USTelecom at page 10.

- Connections between two providers in the call path, which due to technical limitations or misconfiguration cause the Caller-ID to be incomplete (such as just an area code) or to be invalid (such as 0000000000).
- Calls from international numbers where the call is not explicitly indicated as international, resulting in a caller-ID which has too many digits or too few digits to be a valid North American number, OR has the right number of digits but "looks like" an invalid area code or unassigned number.

In an ideal world, all of these situations would get corrected, but this has been going on for decades and is so prevalent that it will take years to fix. To give some perspective, bear in mind that in the SS7 signaling system (at the core of our traditional PSTN), inclusion of Caller-ID is OPTIONAL – so the industry has been less than diligent about making sure it is correct. (On the other hand, the destination number – the number being called, or the TO number – MUST be correct if the call is to complete, so plenty of attention is paid to that.) While some calls include other data items (beyond what we traditionally refer to as Caller-ID) that may indicate the origin of the call, none are consistently available and reliable enough to be used for "spoofed call" filtering.

There is no question that if implemented by all providers, the proposed blocks would ensnare many, many thousands of legitimate calls, and perhaps millions, every day.[19] Given this cost, and

[19] We asked two Strike Force members – Inteliquent and AT&T – to partner with us to audit a representative day's worth of recent call records, to get a more accurate estimate of the legitimate calls that would be blocked by the NPRM filters. Page 1 of the Strike Force October 2016 report says that "The Strike Force is committed to protecting customers" but both of these members declined to invest the several hours of time it would have taken to provide some additional valuable insight here. AT&T did, however, verify signaling anomalies on a small set of selected calls.

the fact that only a tiny fraction of illegal robocalls would be blocked (and only briefly, until the robocallers adapted), the Invalid Number components of the NPRM must be discarded.

IV. Further Input on the Notice Of Inquiry

With billions of calls monthly the robocall epidemic requires mitigation efforts that can operate on a large, sustainable scale. Downstream blocking – that is, intercepting calls after they are already dispersed into the network – will never succeed as long as robocallers are able to place calls at tremendously high rates and to spoof on each call a calling number of their choosing.

While virtually all commenters expressed some level of "support" for the NPRM, the discussion above highlights numerous pitfalls and shows that it will not yield measurable results. A very different approach is necessary.

We concur with the Comments of Sprint in their Section IV, Framework for Evaluating the Effectiveness of Robocalling Mitigation Proposals: "The eventual aim of any work to mitigate robocalling and the use of spoofed caller IDs to perform miscreant acts must be to reduce the incentive to do this to such a point that the issue becomes insignificant, both as to its burden on carriers as well as the nuisance to individual customers."[20]

Sprint identifies four criteria for evaluating mitigation approaches:[21]

1. What reduction in spoofing will this tool allow?
2. How easy is it for the robocallers to continue to place unwanted calls while avoiding the traps placed by any particular tool?

[20] Comments of Sprint Corp. at page 6.
[21] Ibid, page 7

3. What is the cost to the consumer and legitimate network operators to deploy the tool?
4. What are the other downsides of deployment of the tool, such as prevention of delivery of legitimate calls that are wanted by the recipient?

Sprint summarizes with these remarks: "Overall, a more fruitful approach to the robocalling problem is to determine how much mitigation is required to reduce the spoofed robocalling problem to insignificant levels and to examine how all available tools can be assembled to enable such mitigation, rather than examining the merits of each individually and trying to determine how the Commission's rules should be adjusted to enable or even require the use of each on its own. The ability of the bad actors to avoid the impacts of each tool, both alone and in concert with others, must be weighed against the cost to the industry and ultimately to the consumer of their implementation."[22]

Sprint's criteria 1 calls for quantification of the anticipated results from any proposed solution; we have noted repeatedly that this has been woefully lacking thus far. Similarly, proposals to date have failed to present any data or even substantive discussion of the other three Sprint criteria. Moving forward, we must be much for diligent and think, as a group, more critically.

A. Screening, Traceback, Honeypots and Enforcement are Better Tools for Robocall Mitigation

The NPRM asks at 30: "What other methods can be or are used? In particular, we seek comment on the extent to which information obtained through traceback efforts is, can, and should be used to identify future calls that are illegal to a reasonably high degree of certainty?"

[22] Ibid, page 7

The most effective method of addressing illegal robocalls, by all four of the Sprint metrics, is to stop them at the source. Traceback is the most effective technique to find that source. In their Comments, USTelecom makes repeated references to stopping calls at their source, including: "USTelecom maintains that enforcement is ultimately the most effective deterrent to robocalls, since it literally addresses the problem at its source."[23]

There are at least four key elements that will contribute to an effective effort to stop calls at the source: screening by originating providers; improved cooperation among all providers in an optimized and properly facilitated traceback process; integration of complaint data, including honeypots; and further empowerment of regulators to exercise their enforcement obligations. These are discussed in turn here.

Originating Providers need to take responsibility – and to be *mandated* to take responsibility if they won't do it on their own initiative – to limit the ability of illegal robocallers to ply their trade. This does not require large technology investments. Robocall campaigns are characterized by many calls in rapid succession, generally of short duration, increasingly "from" varying telephone numbers. In the internet age, making such capacity available is inexpensive, so Originating Providers do it, as long as the customer pays the (relatively low) bill.

But that doesn't mean that they MUST offer that capability. Guns and ammunition are not necessarily expensive, but there are laws about who is allowed to buy them and what hoops they have to go through to get them. Just as it might be required that a gun dealer do some vetting of his prospective customer before selling an assault rifle that fires 600 rounds per minute, an anonymous visitor shouldn't be able to simply access a service provider's web site

[23] Comments of USTelecom, page 6.

and acquire a SIP trunk that delivers the capability to place 600 phone calls per minute (and to do so using any caller-ID of that anonymous customer's choosing).

The Commission needs to pursue rules that compel originating providers to be more judicious in whom they arm. Technology already exists to limit calls-per-second and number of concurrent calls; providers are also able to audit call records to find abuse. Rules should apply immediately to newly-provisioned customers, and be phased in over time for existing customers. Spoofing capability should be granted only to those that document a demonstrable need; others should be constrained to using provider-verified calling line IDs.

Traceback has to happen better, quicker and cheaper, so that existing sources of robocalls can be found and contained. All service providers (originating, transit and terminating) need to be encouraged – and in fact compelled – to participate in traceback efforts.

Today's traceback efforts are impeded by providers' feigned concern regarding restrictions on release of CPNI, despite an explicit exemption in the law permitting them to share. The FCC needs to flip the balance so that *all providers* respond promptly to good-faith requests for information related to likely illegal robocall campaigns when those requests come from bona fide organizations. Inter-organizational confidentiality concerns should be addressed by specific agreements between the parties.

In their Comments, USTelecom discusses at length the importance of sharing CPNI for traceback efforts, and the need to remove any remaining barriers to such sharing. They say, "In addition to interpreting Section 222(d)(2) to permit the sharing of CPNI, the Commission should also encourage such sharing between providers."[24]

[24] Comments of USTelecom, page 21.

Traceback should be facilitated by an entity charged with this mission and armed with database and productivity tools, available at modest cost, using a continuous improvement process and collaborative efforts to further streamline traceback efficiency and responsiveness, The effort can use the USTelecom model as a starting point.

Robocall complaints roll into the federal agencies (FTC, FCC) at a rate greater than 10,000 per day, and yet there does not appear to be any systemic approach to using this data to rapidly feed traceback and enforcement actions.

Similarly, honeypots (telephone numbers specifically set up to receive and record robocalls) are capturing egregious violations of calling rules, yet appear to be underutilized in the war we're supposed to be fighting. The recordings made by honeypots are tremendously useful because they provide direct evidence of violations (by virtue of recording the announcements played by the robocallers), eliminating any uncertainty introduced by a human complainant operating from memory.

Complaint and honeypot data need to be used to prioritize mitigation efforts so that the highest volume robocalling campaigns get focused resources. Surprisingly, we did not find other commenters highlighting the power of honeypots.

Recent FCC enforcement actions highlight that illegal robocallers, both inside and outside the United States, can be quashed. The current process is grueling – and the longer it takes, the more millions of calls a given campaign can dispatch. FCC enforcement efforts should be generously resourced so that recent successes can be scaled up. Industry should be collaborating on these efforts to an ever-greater extent, and regulations should be in place to encourage that cooperation. Enforcement not only stops the direct target of the enforcement action but it serves as a critical deterrent to others who today operate with little fear of being caught.

The FCC has a mandate to enforce the TCPA. There should be a priority on doing whatever it takes to meet that mandate. As long as the robocall complaint rate is increasing, the FCC is failing.

B. A Provider Safe Harbor Should Incent Stopping Robocallers at the Source

The NPRM at 34-36 asks about potential Safe Harbors. Many commenters volunteered support for a safe harbor allowing providers to block calls pursuant to the NPRM. We've made clear that such blocking is ill-advised; correspondingly a safe harbor for such blocking would not be appropriate.

The NPRM, and most of the commenters, fail to distinguish between Originating Providers versus Transit and Terminating providers. These are critical distinctions and need to be incorporated into any thinking about blocking practices.

The Originating Provider is the one closest to the robocaller, and thus the one in the best position to stop the calls before they are dispersed further into the PSTN. Originating Providers should be taking proactive steps to limit the rates at which their customers can place calls, and to contain the caller-ID values that their customers can assign to those calls. For select customers, Originating Providers will need to relax their rules and should do so via a documented process that includes vetting the customer, understanding their particular needs for caller-ID and/or call-rate flexibility, and mechanisms to insure on-going compliance with less-restrictive limits.

An Originating Provider in compliance with this approach should earn safe harbor status; otherwise, they should face liability as the "caller" for prohibited calls under TCPA and related statutes and regulations.

Downstream providers (Transit and Terminating Providers), as a general rule, should not be permitted to block calls on their own initiative. Terminating Providers should be able to block or otherwise route calls according to whatever wishes are communicated to them by the terminating end-user. If a provider DOES block a call, they should be required to play an appropriate announcement to the calling party.

C. There Needs To Be A Robocall Czar

Our favorite remark in all of the Comments in this docket comes from Louis Taff. He asks: "[D]oes anyone own this problem?"[25] We believe the current answer is No, and that's not good.

The Robocall Strike Force showed some promise, but in the eight months since it published its first report in October of 2016, the number of robocall complaints per month (at the FTC) has increased, not gone down. In its first at-bat, the Strike Force struck out.

We believe the industry needs to be more explicit about its commitment of resources to this problem (and prioritizing the application of those resources according to criteria such as those espoused by Sprint).

The FCC has declared the war on robocalls a priority. In the FCC's 2018 Budget Proposal, the agency lists "3.1.1 Implement proposals to target and eliminate unlawful

[25] Comments of Louis Taff, page 3. Available at https://ecfsapi.fcc.gov/file/1062970610984/Taff-comments-on-FCC-doc-17-24.pdf

robocalling" under its Strategic Objective 3.1.[26] But there's no further mention of robocalling in the document. The FCC should be clear what part of its $300 million spending plan is allocated to this particular priority, and how many FTE's are assigned – and who they are.

The FCC, with input from industry, should appoint a Robocall Czar to shepherd the collecting and vetting of potential mitigation techniques and the prioritization of the industry and government resources. This needs to be an iterative, interactive process that welcomes input from "outsiders" rather than the insular process employed by the Strike Force effort.

Quantitative metrics must be established to gauge results and guide further actions. Such measures will determine if the Czar is a hero or a goat.

V. Concluding Comments

We all agree that robocalling is a huge problem. Many say that there is no silver bullet, telling us that the answer is a broad portfolio of solutions. But for a problem of this scale, nibbling at the edges will not have a measurable impact. In fact, efforts such as those in the NPRM, while well-intentioned, will only serve as distractions.

We have identified here steps that WILL make a difference if executed with diligence and commitment. These are not technologically complex or resource-intensive (relative to the scope of the problem), and they can be implemented starting now. The most effective role for the Commission is to:

1. Facilitate industry cooperation through the appointment of technically competent, committed leadership tasked with prioritizing resources and coordinating investments

[26] FCC Fiscal Year 2018 Budget Estimates to Congress, May 2017, page 56. Available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-344998A1.pdf

to provide the highest level of illegal robocall mitigation for the lowest cost in the shortest time.

2. Obligate providers to be “good guys” in the fight against illegal robocalls, or risk enforcement action as the perpetrator of such calls.
3. Continue, and scale, your enforcement efforts to not only directly stop the biggest violators but to send a message to others that they will be caught and penalties will be harsh.

We can expect every provider to resist any outsider telling them what to do. They will always agree with anything that grants them permission without obligation. But the industry has demonstrated that despite their own assurances that on their own initiative they’re doing everything that can be done, they are not. Time for a bigger stick.

The FCC’s oversight, regulatory and enforcement powers, applied in a judicious and focused manner, can turn the tide on this seemingly intractable problem.

Respectfully submitted,

DATED: 24 July 2017

/s/ David Frankel

dfrankel@zipdx.com
Tel: 800-372-6535

APPENDIX A

Telephone Numbers in the United States Public Switched Telephone Network (PSTN)

This appendix presents an explanation of how telephone numbers are handled in our PSTN, with an emphasis on how the information about the "calling line ID" is passed to the called party. The content here is technical, as the nuances of the technology bear heavily on what the called party sees and on the data items available as the call is processed, should a provider wish to intercept it. However, we note that we have omitted many details (including technical references) for brevity and instead focused on items most relevant to the NPRM and its implications for our existing and future telephone networks.

PROVIDERS: A telephone call is handled by one or more providers:

- The Originating Provider (**OP**), the provider that accepts the call from the end-user initiating the call.
- The Terminating Provider (**TP**), the provider that delivers the call to the called party.
- Zero or more Transit Providers and/or Inter-Exchange Carriers (**XP**) carry the call between the OP and the TP. The OP and the TP may be the same, or they may be directly connected, in which case there will be no XP.

For example: Sally, a Frontier wireline customer in Connecticut, calls Bob, a T-Mobile Wireless customer in Oregon. Frontier hands Sally's call to CenturyLink, an XP, because Frontier is not directly connected to T-Mobile. CenturyLink carries the call across the country and hands it to Inteliquent, another XP, which in turn passes it to T-Mobile.

Frontier is the OP, CenturyLink and Inteliquent are XPs, and T-Mobile is the TP.

PROTOCOLS: Almost all telephone calls worldwide are established using digital protocols that provide for message exchanges containing several data items. Placing a phone call involves sending a message that includes: who the call is directed TO (the callED party); who it is FROM (the callING party); and other technical details. There are three protocols that are most widely used:

- **ISUP** is the oldest of the three and is widely used in traditional wireline networks. ISUP is part of the broader SS7 protocol family. There are multiple variants; the ANSI version is used in North America and the ETSI version prevails elsewhere.
- **GSM** is used for over-the-air communications between a handset and a base station (cell tower).
- **SIP** is used in newer IP-based networks and in some wireless implementations.

NUMBER FORMATS: In the United States, we use the North American Numbering Plan (**NANP**), which is a 10-digit area code, prefix and number format (NPA-NXX-XXXX). Each country around the world defines their own numbering plan. Some have more digits, some have fewer. In some countries, numbers can vary in length. Within a given country, any given subscriber's number is referred to as a "national number."

The **ITU**, an agency of the United Nations, maintains the E.164 specification that assigns a "Country Code" to each country. The country code, in combination with the "national number" defines a complete number that is unique in the world.

A string of digits that includes the country code is an International Number.

The Country Code for the USA is 1; we share this Country Code with a few other countries (including Canada), which are members of the NANP. By assigning unique area codes to different parts of the NANP, we can maintain the uniqueness of these numbers.

Most Country Codes are two digits: France is 33, UK is 44, China is 86, India is 91, Australia is 61. Some are three digits: Bulgaria is 359 and Hong Kong is 852.

DIAL PLAN: A dial plan specifies how the dialed string of digits will be interpreted when a call is placed. From most phones in the USA, if we first dial a “1”, the dial plan will infer that the next 10 digits will be a NANP National Number – that is, an area code, prefix, and number. If we first dial “011” then the dial plan infers that we are dialing an International Number (and thus the 1, 2 or 3 digits immediately following 011 will be a country code).

In many places in the United States, we can omit the 1 and just dial 10 digits; the dial plan assumes this is a National Number. In some locations, you can dial just 7 digits and the dial plan will assume you are placing a call to the same area code from which you are originating the call.

Many mobile phones allow you to dial a “+” or to include “+” in your contact list. When a number starts with “+” the dial plan interprets what follows as an international number. Thus, in many cases, dialing 1-612-555-1234 or +16125551234 or just 612-555-1234 would be interpreted as a call to Minnesota. But dialing 011-612-555-1234 or +612-555-1234 would be a call to Australia because the country code for Australia is 61. The dialing plan ignores dashes.

Many business telephone systems (PBX’s) have their own dialing plans. They may permit the dialing of just 3 or 4 or 5 digits to reach another extension within the building or on the campus. They may have special codes for extensions at remote locations. And they often require dialing a “9” before calling a number external to the organization, to reach a national or international number. Similarly, different countries have their own dialing plans for distinguishing national and international numbers. Where in the US we tend to use 1 as a prefix for national calls and 011 for international, many other countries use 0 for national calls and 00 for international.

When a telephone user places a call, the network receiving the call and the user must have a shared understanding of the dialing plan to be used. If Sally is at home, she probably dials 503-555-1234 to reach Bob. From her office, she might dial 9-1-503-555-1234. Her mobile phone might have a flexible dialing plan that allows her to put 1, +1, or nothing in front of the 503. If she travels to France, she’ll have to dial 00-1-503-555-1234 from a landline.

RE-ORIGINATION: As a call gets passed along from the calling party to the OP and then from the OP to XP, XP to XP, XP to TP, TP to the called party, it is “re-originated” – that is, a new signaling message is generated and sent onward at each hop, using the signaling data that was received. As each successive provider initiates the next hop, it has to know what dialing plan is expected and, if necessary, modify the number(s) it sends.

In the ISUP protocol, there are indicators associated with the Called Party Number and the Calling Party Number that specify whether the number is a “national number” or an “international number.” But often, these indicators are ignored and the two ends just agree on some convention (such as: “We shall agree to assume a dialed number is a national number unless it starts with 011”).

Calls may arrive at an XP with the ETSI variant of ISUP, but get sent onward using the ANSI variant. Due to differences in the protocols, the data may not be transferred precisely or consistently.

Sometimes, when a provider re-originates a call, it will drop the indicators or set them incorrectly. In SIP, a number is supposed to start with + if it is an international number. But some carrier dialing plans don't accept a +, so if it is present, it may get removed.

Providers exchange calls with each other over **trunks**; a given trunk can carry multiple calls simultaneously. Some trunks may be designated as "international" or dedicated to calls from a specific country, helping the receiving provider interpret the calling number. But when a call is re-originated onto the next hop, that next trunk likely doesn't carry the international or country-specific designation on which the call arrived. This can add to the confusion.

Defects in how the Calling Number (FROM) is passed onward are quite prevalent, because even if the Calling Number is set incorrectly, the call will typically still go through as long as the Called Number (TO) is valid.

INTER-WORKING: If a call arrives via ISUP and must go onward via SIP, then it has to be inter-worked; that is, converted from one protocol to another. The IETF publishes a document, RFC3398, that prescribes how this can be done. Section 12 of this document details how national and international numbers are converted back and forth.

The beginning of the document says "This mechanism *might* be implemented when using SIP in an environment where part of the call involves interworking with the Public Switched Telephone Network (PSTN)." We have added the emphasis to make the point that generally, this mechanism is NOT implemented. Each equipment manufacturer makes their own decisions about how to implement the inter-working, Sometimes manufacturers allow the network operator to select how it gets done. So, instead of the consistent treatment of numbers that would apply if the RFC3398 were followed consistently, there are a wide variety of formats in use. They are not always predictable.

WHY BLOCKING FAILS: By the time a call has propagated at least partway through the network, it becomes a matter of informed guesswork to interpret the Calling Number. For example:

- Sally calls Bob from her landline and the Calling Party Number gets passed along as 2032346000. That looks like a good national number.
- Sally calls from her mobile, and the Calling Party Number is 12034566000. That's a good NANP-compliant international number.
- Sally calls from the office, extension 403. The Calling Party Number contains just 403, because her PBX failed to send the full national number when it passed her call to Frontier, and Frontier just passed what it got when it re-originated the call to the next hop. The number is "invalid" as a NANP number and thus could get blocked by CenturyLink or Inteliquent or T-Mobile. Potentially all calls from this PBX could be blocked.

- Sally travels to Belgium and calls Bob from her office there, where her office (FROM) phone number is 2 588 4364. This time the OP is Belgacom; they send the call to AT&T, which realizes it came from Belgium and so prefixes the country code 32 ahead of the number before re-originating it to T-Mobile, with whom it has a direct connection, T-Mobile gets the calling number as 3225884364. It looks like a NANP national number, but 322 is not a valid area code, so T-Mobile potentially blocks the call. All calls from Brussels could be blocked.
- Sally travels to the office in Paris and calls from there; her calling number is 33180141689. That's a valid number in France but has too many digits to be a NANP number, so T-Mobile potentially blocks it. There's no certainty that such numbers will be marked as "international" or will be prefixed with a + when they are re-originated or inter-worked, so vast numbers of international calls could be blocked.
- Sally returns home with her colleague Pierre. He calls Bob using his French mobile phone with a +33 French caller-ID. Because he is in the US, his call is sent over a domestic trunk and his number appears invalid. His call is blocked. All foreign visitors roaming in the US could have their calls blocked – not the ideal welcome mat.
- Sally goes to her country house; the community has a very old telephone switch. When she places her call to Bob, no calling party information is sent. When Inteliquent finally gets the call and passes it on to T-Mobile, they fill in 0000000000 because their equipment won't process a call with a blank FROM field. 0000000000 is invalid, so T-Mobile blocks the call. If everybody implements this kind of blocking, nobody in this rural community will be able to make a phone call.

THE FIX: Because there are hundreds of thousands of switches and connections between and among the various providers (in the US alone), it is not practical to think that we'll have a universal fix for this anytime soon. There is no way blocking practices as described in the NPRM could be broadly implemented without massive disruption to on-going telephone traffic. And if the blocks are implemented very narrowly, as they would have to be, then they would be even less effective at stopping a measurable number of illegal robocalls.