

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

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	CG Docket No. 02-278
Telephone Consumer Protection Act of	)	
1991	)	
	)	
Establishing Just and Reasonable Rates for	)	WC Docket No. 07-135
Local Exchange Carriers	)	
	)	

**COMMENTS OF  
THE UNITED STATES TELECOM ASSOCIATION**

Kevin Rupy  
B. Lynn Follansbee  
Jonathan Banks

United States Telecom Association  
607 14th Street, N.W.  
Suite 400  
Washington, D.C. 20005  
(202) 326-7271

January 23, 2015

**TABLE OF CONTENTS**

**I. Do-Not-Call Violations Negatively Impact Consumers and Carriers. .... 2**

**II. Effectively Addressing Unwanted Telemarketing Calls Raises Complex Issues..... 5**

**A. A Diversity of Robocall Mitigation Options Exists Under the Commission’s Current Legal Framework..... 6**

**B. Comprehensively Addressing Do-Not-Call Violations is a Technologically Challenging Endeavor. .... 11**

**1. The Significance of Transitioning to Full-IP Networks..... 12**

**2. The Challenge of Caller-ID Spoofing. .... 14**

**3. Carrier Limitations on Visibility Into Network Traffic. .... 16**

**III. Consumers Today Can Access an Expanding Assortment of Services From a Broad Range of Providers to Mitigate Do-Not-Call Abuses. .... 17**

**IV. Conclusion..... 20**

\* \* \*

## SUMMARY

The letter from the National Association of Attorneys General raises issues regarding the legal, practical and technological challenges that may arise regarding the implementation of certain call-blocking technologies by common carriers to address the problem of robocalls. USTelecom welcomes this discussion since we share many of the same concerns raised by NAAG and others regarding abuses of the Do-Not-Call framework. USTelecom continues to work cooperatively with a broad range of stakeholders on this issue in order to find a practical, workable solution to the problem of telephony abuse and fraud resulting from unwanted, and sometimes unlawful, robocalls.

USTelecom understands and shares the widespread frustration resulting from violations of the Do-Not-Call framework. Such calls are not only an annoyance, but criminal elements can at times exact financial and emotional harms upon unsuspecting or vulnerable consumers. Given the realities of today's competitive marketplace, carriers must develop and deploy effective tools that might operate to mitigate annoying – and at times, criminal – robocalls in order to retain their customers and stave off potential competitive alternatives. But in addition to the harm many robocalls cause consumers, these unwanted calls impact USTelecom's own member companies. In addition to dedicating significant customer service and fraud response resources towards this issue, these calls can also adversely impact our companies' networks. In extreme instances can degrade and disrupt services in a provider's impacted area.

As acknowledged by the Commission in its Notice, there are a number of issues arising from the ongoing battle to address unwanted telemarketing calls. Among them, the extent to which regulated common carriers can proactively and privately decide to block network traffic associated with the making and receiving of calls. Carriers are generally not permitted to engage in call blocking except in rare circumstances. However, USTelecom agrees with the Commission's determination that its precedent has no effect on the right of "individual end users" to choose to block incoming calls from unwanted callers at the end user's premises or device.

There are also inherent technological challenges associated with effectively addressing this issue. These include the widespread abuse of caller ID by bad actors and the real-time nature of abusive calls. A fundamental challenge facing all stakeholders, however, is that existing time division multiplexing (TDM) networks are less robust than more advanced IP networks with respect to their current and future ability to support advanced anti-robocall solutions.

In the face of these challenges, consumers today have access to a broad range of services designed to aid them in managing annoyances and harms, including those that may result from abuses of the Do-Not-Call framework. These services are available through a broad range of providers, including independent application developers, telecommunications carriers and equipment vendors. USTelecom shares the view of many other stakeholders that no single 'silver bullet' exists today that will comprehensively solve the problem.

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

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	CG Docket No. 02-278
Telephone Consumer Protection Act of	)	
1991	)	
	)	
Establishing Just and Reasonable Rates for	)	WC Docket No. 07-135
Local Exchange Carriers	)	
	)	

**COMMENTS OF  
THE UNITED STATES TELECOM ASSOCIATION**

The United States Telecom Association (USTelecom)<sup>1</sup> submits these comments in response to the Public Notice (Notice) released by the Federal Communications Commission (Commission) in the above-referenced proceedings.<sup>2</sup> Through its Notice, the Commission seeks comment on a letter it received from the National Association of Attorneys General (NAAG) that formally requests an opinion regarding phone companies' legal ability to implement call-blocking technology (NAAG Letter).<sup>3</sup>

The NAAG Letter raises issues regarding the legal, practical and technological challenges that may arise regarding the implementation of certain call-blocking technologies by common carriers to address the problem of robocalls. USTelecom welcomes this discussion since we

---

<sup>1</sup> USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

<sup>2</sup> Public Notice, *Consumer and Governmental Affairs Bureau Seeks Comment on Robocalls and Call-Blocking Issues Raised by the National Association of Attorneys General on Behalf of Thirty-Nine Attorneys General*, DA 14-1700 (released November 24, 2014) (*Notice*).

<sup>3</sup> See, Letter from the National Association of Attorneys General, to FCC Chairman Tom Wheeler, dated September 9, 2014 (*NAAG Letter*).

share many of the same concerns raised by NAAG and others regarding abuses of the Federal Trade Commission's (FTC) Do-Not-Call framework. USTelecom continues to work cooperatively with a broad range of stakeholders on this issue in order to find a practical, workable solution to the problem of telephony abuse and fraud resulting from unwanted, and sometimes unlawful, robocalls.

USTelecom has long been involved in addressing the significant consumer and government concerns resulting from violations of the Do-Not-Call framework jointly administered by the Commission and the FTC. USTelecom's member companies understand and appreciate the annoyance and potential monetary harms inflicted on consumers and businesses resulting from these violations. Our industry has a long track record of working with consumer, industry and regulatory stakeholders on ways to mitigate such harms, and has developed strong relationships with law enforcement agencies at the local, state and federal level.

**I. Do-Not-Call Violations Negatively Impact Consumers and Carriers.**

USTelecom understands and shares the widespread frustration resulting from violations of the Do-Not-Call framework. Such calls are not only an annoyance, but criminal elements can at times exact financial and emotional harms upon unsuspecting or vulnerable consumers. Given consumers' increasing irritation with receiving unwanted calls, there is tremendous pressure on wireline carriers to offer services and tools to their subscribers in order to retain their patronage and good will in addition to mitigating harms that might befall them.

Given the realities of today's competitive marketplace,<sup>4</sup> carriers must develop and deploy effective tools that might operate to mitigate annoying – and at times, criminal – robocalls in order to retain their customers and stave off potential competitive alternatives. The competition between our member companies and other communications platforms for consumer and enterprise business provides incentives for all communications providers to innovate and to develop new and more effective solutions to these challenges. If we do not offer such solutions, consumers will simply turn to alternate technologies and providers that offer better ones.

But in addition to the harm many robocalls cause consumers, these unwanted calls impact USTelecom's own member companies. Often, the first call a consumer makes seeking assistance to address annoying calls is to the phone company. Our member companies' customer service representatives represent the first line of defense, and must be well versed in explaining to customers the difference between legal and illegal calls, pointing them to tools available to help them avoid or manage these calls and providing them with information on how to file a complaint with the FTC.

These calls can also adversely impact our companies' networks. In some instances, robocalls calls may appear on the networks as 'mass-calling events', which are typically highly

---

<sup>4</sup> Among telephone households during 2013, more than 90 percent had wireless service and 43 percent used only wireless telephones for voice service. In remaining telephone households, 30 percent were using non-traditional services such as VoIP via broadband, predominantly from cable companies. This means only 27 percent of telephone households were using traditional landlines as of year-end 2013. When taking into account customers who have both wireless and landline phones, but use their wireless phones mostly, USTelecom projects that the portion of customers relying either exclusively or mostly on traditional landlines will be only 11 percent by the end of 2015. Based on national trends, by the end of 2015, the portion of telephone households at the national level using only wireless phones for voice service is projected to surpass 50 percent. See, USTelecom website, Consumers Continue Shift Away From Landline – Regulations Are Behind, November 25, 2014 (available at: <http://www.ustelecom.org/blog/consumers-continue-shift-away-landline-%E2%80%93-regulations-are-behind>) (visited January 23, 2015).

localized, tremendously high volume, and extremely brief – lasting only a matter of minutes. And providers receive no advance warning of these calls. A severe mass-calling event can result in service degradation and disruptions to phone services in a provider’s impacted area. Moreover, illegal robocalls exacerbate an already troubling economic problem in our industry because they can often be associated with “phantom traffic” – calls largely originating outside our companies’ local calling areas for which a terminating access charge will never be paid by the long-distance carrier because the necessary call identification information has been substituted or stripped.

Finally, because these calls may sometimes involve criminal matters impacting their customers, most larger carriers have established call fraud bureaus. For example, many USTelecom member companies maintain network operations centers (NOCs), which include 24-hour security desks that monitor network traffic, respond to consumer complaints, conduct traffic data forensics, and initiate mass calling investigations.

Carriers will initiate legal actions against appropriate parties when they can be found and routinely coordinate with law enforcement agencies at the state and federal level during ongoing investigations and enforcement actions. For example, in a 2010 FTC action against a robocaller that allegedly made more than 370 million calls to consumers nationwide in a single year, the agency specifically acknowledged the assistance that both AT&T and Verizon provided in the investigation of the case.

In instances where such calls are part of a mass calling event, carriers may be in a position to provide the Commission, FTC and other industry stakeholders with crucial forensic information related to these calls. USTelecom encourages the Commission to identify what kind of information it would find helpful in this regard, and explore whether there are procedures that

could be implemented to streamline the sharing of information with appropriate enforcement agencies, and perhaps other carriers. By doing so, industry and government stakeholders may be able to streamline and improve the ability of all impacted parties to act more expeditiously on this information.

## **II. Effectively Addressing Unwanted Telemarketing Calls Raises Complex Issues.**

As acknowledged by the Commission in its Notice,<sup>5</sup> there are a number of issues arising from the ongoing battle to address unwanted telemarketing calls. Among them, the extent to which regulated common carriers can proactively and privately decide to block network traffic associated with the making and receiving of calls. Through a series of decisions dating back 25 years, the Commission has established legal precedent that “no carriers . . . may block, choke, reduce or restrict [telecommunications] traffic in any way.”<sup>6</sup> This general prohibition has no effect on the right of individual end users to choose to block incoming calls from unwanted callers.<sup>7</sup>

Beyond the realities of the Commission’s call blocking precedents, there are also inherent technological challenges associated with effectively addressing this issue. The challenges have been acknowledged by a broad range of parties involved in efforts to mitigate these calls,

---

<sup>5</sup> Notice, pp. 2 - 4.

<sup>6</sup> See, Declaratory Ruling and Order, *Establishing Just and Reasonable Rates for Local Exchange Carriers*, DA 07-2863, ¶ 6 (released June 28, 2007) (*Declaratory Ruling*). See also, Memorandum Opinion and Order, *Blocking Interstate Traffic in Iowa*, FCC 87-51, 2 FCC Rcd 2692 (1987) (*Iowa Blocking Order*); see also, Report and Order and Further Notice of Proposed Rulemaking, *Connect America Fund*, 26 FCC Rcd 17663, FCC 11-161, ¶ 734 (released November 18, 2011) (*USF Order*); see also, Declaratory Ruling and Order, *Policies and Rules Concerning Operator Service Providers*, DA 13-1990, ¶¶ 8 – 9 (released September 26, 2013) (*Operator Service Order*); Declaratory Ruling, *Developing an Unified Intercarrier Compensation Regime*, DA 12-154 (released February 6, 2012) (*Rural Call Completion Order*);.

<sup>7</sup> *Declaratory Ruling*, n. 21.

including government and industry stakeholders.<sup>8</sup> While some of these challenges are daunting – most notably the widespread prevalence of caller identification (caller ID) spoofing – a diverse group of stakeholders, including carriers, have deployed various technological solutions that can and do help their customers reduce and manage the negative impact of these calls.

**A. A Diversity of Robocall Mitigation Options Exists Under the Commission’s Current Legal Framework.**

Carriers are generally not permitted to engage in call blocking except in rare circumstances. In a series of decisions dating back to 1987, the Commission has generally concluded that call blocking is an unjust and unreasonable practice under section 201(b) of the Communications Act of 1934, as amended (the Act).<sup>9</sup> In the first such instance, the Commission stated that “the blocking of interstate traffic . . . was in violation of the Communications Act and Commission policy.”<sup>10</sup>

In its more recent decisions, the Commission has continued to make clear that common carriers may not block calls, and indeed may be held liable for acts or omissions, by themselves or their agents, that impede call completion. For example, in 2007, the Commission, on its own motion, issued a Declaratory Ruling to “remove any uncertainty about the scope of the Commission’s general prohibition on call blocking,” and to clarify the obligation of certain types of carriers to “complete their customers’ interexchange calls.”<sup>11</sup> In its order, the Commission stated that it “has been, and remains, concerned that call blocking may degrade the reliability of

---

<sup>8</sup> See generally, Transcript, Federal Trade Commission Summit, *Robocalls All The Rage* (October 18, 2012) (*FTC Transcript*) (see e.g., comments of FCC Chief Technologist Henning Schulzrinne. *FTC Transcript*, pp. 17 – 42). See also, comments of Adam Panagia, director of AT&T's Network Fraud Investigation. *FTC Transcript*, pp. 126 – 136. See also, Comments of Kevin Rupy, Senior Director of Policy, USTelecom. *FTC Transcript*, pp. 44 – 51.

<sup>9</sup> See, note 6, *supra*.

<sup>10</sup> See, *Iowa Blocking Order*.

<sup>11</sup> *Declaratory Ruling*, ¶ 1.

the nation's telecommunications network.”<sup>12</sup> The Commission reiterated that its “precedent provides that no carriers, including interexchange carriers, may block, choke, reduce or restrict traffic in any way.”<sup>13</sup>

Then, in its 2011 Universal Service Fund Order, the Commission considered the question of whether it would permit carriers in the call path to block traffic that is unidentified or for which parties refuse to accept financial responsibility.<sup>14</sup> The Commission ultimately concluded that it would “decline to adopt any remedy that would condone, let alone expressly permit, call blocking.”<sup>15</sup> After reiterating its “longstanding prohibition on call blocking,” the Commission emphasized its belief that “call blocking has the potential to degrade the reliability of the nation's telecommunications network.”<sup>16</sup> In doing so, the Commission noted that “call blocking ultimately harms the consumer, whose only error may be relying on an originating carrier that does not fulfill its signaling duties.”<sup>17</sup>

Subsequently in 2012, the Commission released a Declaratory Ruling in its Rural Call Completion proceeding to clarify the scope of its prohibition on blocking. The Commission noted that instances of call blocking can have “dire consequences,” including small businesses “los[ing] customers who get frustrated when their calls don't go through,” “[u]rgent long distance calls from friends or family” being missed, and “those in need of help” being “unable to reach public safety officials.”<sup>18</sup>

---

<sup>12</sup> *Id.*, ¶ 5.

<sup>13</sup> *Id.*, ¶ 6.

<sup>14</sup> *USF Order*, ¶ 734.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Rural Call Completion Order*, ¶ 2.

After reminding carriers of its “longstanding prohibition on carriers blocking, choking, reducing or otherwise restricting traffic,”<sup>19</sup> the Commission further explained the scope of this prohibition. It clarified that “practices that lead to call termination and call quality problems may constitute unjust and unreasonable practices in violation of section 201 of the Act, and/or may violate a carrier’s section 202 duty to refrain from unjust or unreasonable discrimination in practices, facilities, or services.”<sup>20</sup> It further emphasized that, under the Act, “carriers are responsible for the actions of their agents or other persons acting for or employed by the carriers.”<sup>21</sup>

In all circumstances in which the Commission has identified unreasonable motivations behind carrier call-blocking practices, it has identified potential adverse consequences of those practices. These potential adverse consequences could presumably occur whenever any form of call blocking is employed in a carrier network for any reason. However, USTelecom agrees with the Commission’s determination that its precedent has no effect on the right of “individual end users” to choose to block incoming calls from unwanted callers at the end user’s premises or device. To be clear, the Commission’s precedent establishes an affirmative right for “individual end users” to choose to “block incoming calls from unwanted callers.”<sup>22</sup> However, the same precedent makes clear that carriers may not “block, choke, reduce or restrict traffic *in any way*.”<sup>23</sup> This has created a statutory framework whereby phone companies deploying call mitigation technologies must generally ensure they do not inadvertently block, choke, reduce or

---

<sup>19</sup> *Id.*, ¶ 3.

<sup>20</sup> *Id.*, ¶ 4.

<sup>21</sup> *Rural Call Completion Order*, ¶ 4.

<sup>22</sup> *Declaratory Ruling*, n. 21.

<sup>23</sup> *Id.*, ¶ 6 (emphasis added).

restrict legitimate traffic in the network, while consumers are free to avail themselves of options to mitigate and/or block any or all incoming calls at the premises.

This has resulted in a diverse ecosystem of services developed by a broad range of providers. These include offerings from carriers that comply with the Commission’s legal framework, as well as offerings from software developers and equipment manufacturers that are generally developed for use by end users at the premises and not as “central office” based network solutions engineered to comply with the Commission’s call blocking precedent.<sup>24</sup>

The end result of this legal dynamic is that carrier offerings to consumers do not indiscriminately block voice services to their respective subscribers. Rather, carriers offer tools that empower consumers to exercise control over their own incoming calls – allowing, refusing, or redirecting them. Such tools can include basic offerings like caller ID that leave the decision on whether to accept or reject a call in the hands of a consumer. They may also offer more robust tools, such as white lists, and do not disturb features, that allow consumers to control when or from whom they will receive a call.<sup>25</sup>

In contrast to the tools offered by carriers, some third-party tools and services – which are not subject to the same call-blocking legal restrictions as carriers – allow consumers to more extensively block a broad range of incoming calls. Increasingly, consumers, third party providers, and some policy makers are asking why these premises-centric solutions cannot be employed within carrier networks; indeed, this seems to be the motivating impulse behind the

---

<sup>24</sup> Specific examples of these services are discussed in Section III of these comments.

<sup>25</sup> See e.g., AT&T website, *U-verse® Voice Support* (available at: <http://www.att.com/esupport/article.jsp?sid=KB401850&cv=814#fbid= udIV86ewq->) (visited January 23, 2015); see also, CenturyLink website, *Calling Features by Plan* (available at: <http://www.centurylink.com/home/phone/>) (visited January 23, 2015); Verizon website, *FiOS Digital Voice Calling Features* (available at: <http://www.verizon.com/home/phone/fiosdigitalvoice/#features>) (visited January 23, 2015).

NAAG letter. Given the different legal obligations for carriers and other types of providers, these premises centric services can sometimes take a more aggressive approach towards the blocking of communications traffic. Such services often rely on black lists to block a universe of calls,<sup>26</sup> and some can take an invasive approach to identifying illegitimate traffic.<sup>27</sup> More recent offerings work across a variety of platforms, including wireless and IP, while others – usually in the form of customer premises equipment (CPE) – are designed to operate on traditional TDM networks.

As a general matter, consumers benefit from competition among diverse providers of robocall solutions. However, while USTelecom takes no position on the capabilities and effectiveness of any particular tools, the Commission should consider whether they raise privacy concerns, and whether the impact of their widespread deployment across the public switched telephone network (PSTN) could have impacts adverse to the public interest.

Specifically, there are no assurances that poorly designed and overly broad technologies would not negatively impact legitimate traffic, even if employed at the premises. Such adverse effects could result from overly inclusive black lists, indiscriminate blocking of carriers' traffic

---

<sup>26</sup> Black list technologies contain a universe of phone numbers that are used to affirmatively block calls containing the phone numbers on the underlying list. Such lists can be populated based on customer feedback (*e.g.*, through a prompt or portal), or through data provided from the Do-Not-Call list maintained by the FTC and some states. In contrast, white list technologies deliver only those phone numbers specified by a customer (*e.g.*, their spouse's work phone number and cellphone number). Any phone numbers not on a customer's white list will be sent to either voice-mail or to a standard message informing callers that the person they are trying to contact is unavailable.

<sup>27</sup> For example, Pindrop Security has proposed that telephony providers expand the use of its PhonePrinting™ technology to consumer applications. Among other things, that technology measures 147 characteristics of an audio signal, and includes analysis of both live and recorded phone calls. *See e.g.*, Pindrop Security White Paper, *Phone Fraud & Social Engineering: How the Modern Thief Robs a Bank*, 2013, p., 10. *See also*, Pindrop Security website, *Fraud Detection System* (available at: <http://www.pindropsecurity.com/fraud-detection-system/>) (visited January 16, 2015) (noting that its fraud detection system “needs approximately 15 seconds of audio to analyze and match a call.”).

by third-party applications,<sup>28</sup> or unanticipated technological glitches that impede legitimate traffic. While marketplace forces may be effective in addressing some of these instances, the Commission has already acknowledged that call completion problems can have “dire consequences.”<sup>29</sup> These consequences can presumably occur wherever blocking technologies are employed.

Moreover, it is unclear what measures – if any – the Commission could take to address instances of call completion abuses stemming from third-party call blocking technologies. For example, at least one third-party call blocking service may be indiscriminately blocking all numbers assigned to a specific carrier that it has identified as a “per se” robocaller.<sup>30</sup> If such extrajudicial practices were widely adopted by other edge-based providers offering block list services, its impact on legitimate calls could be significant. Before endorsing any particular solutions in this environment, the Commission should assess such technologies on a data-driven basis.<sup>31</sup>

### **B. Comprehensively Addressing Do-Not-Call Violations is a Technologically Challenging Endeavor.**

Operating within the current legal framework, carriers – and other third-party providers – are continuing to develop and deploy various technologies to empower consumers to control the manner in which they use their voice services. Several technological challenges confront service

---

<sup>28</sup> See, USTelecom Response to Senator Claire McCaskill, p. 9, August 16, 2013 (available at: <http://www.mccaskill.senate.gov/imo/media/doc/RobocallDetailedResponsetoSen%20McCaskill.pdf>) (visited January 21, 2015) (*USTelecom Response*).

<sup>29</sup> *Rural Call Completion Order*, ¶ 2.

<sup>30</sup> See, *USTelecom Response*, p. 9.

<sup>31</sup> See e.g., Federal Communications Chairman Tom Wheeler, *NET EFFECTS: The Past, Present, and Future Impact of Our Networks* (stating that “One key component of the FCC’s administrative process is to focus like a laser on a fact-based, data-driven process.”) (available at: <http://www.fcc.gov/page/net-effects-past-present-and-future-impact-our-networks>) (visited January 21, 2015).

providers in their laudable efforts, including the widespread abuse of caller ID by bad actors and the real-time nature of abusive calls. A fundamental challenge facing all stakeholders, however, is that existing time division multiplexing (TDM) networks are less robust than more advanced IP networks with respect to their current and future ability to support advanced anti-robocall solutions.

### **1. The Significance of Transitioning to Full-IP Networks.**

The reliance of more advanced technological solutions on underlying IP networks raises an important issue central to the challenge of developing more robust tools to effectively address Do-Not-Call violations. The communications industry is in the midst of transitioning from the PSTN – rooted in century-old, fixed-location, voice-centric technology – to mobile and IP based networks.

Widespread deployment of all-IP networks can better facilitate and support tools and services that will benefit consumers in the management of their communications needs and services. Indeed, the Commission has established a policy goal of “accelerat[ing] the transition from circuit-switched to IP networks, with voice ultimately one of many applications running over fixed and mobile broadband networks.”<sup>32</sup> In addition to the massive investment by industry in deploying these networks, the Commission is also in the process of overseeing this transition.<sup>33</sup> The Commission has opened a new proceeding seeking input on how to modernize the Commission’s policies and rules to encourage the IP transition.

---

<sup>32</sup> *USF Order*, ¶ 11

<sup>33</sup> *See e.g.*, Notice of Proposed Rulemaking and Declaratory Ruling, *Ensuring Customer Premises Equipment Backup Power for Continuity of Communications, Technology Transitions*, 80 FR 450, FCC 147-185 (released November 25, 2014). *See also*, Report and Order and Further Notice of Proposed Rulemaking, *Connect America Fund*, 29 FCC Rcd 8769, FCC 14-98 (released July 14, 2014).

The transition to IP networks will promote the development of tools to better manage unwanted calls, including the deployment of secure-call-authentication procedures that can address the problems posed by hidden, disguised, or spoofed calling party telephone numbers more effectively. As noted by the FCC’s former Chief Technologist, we have a “much better chance” of addressing robocalls through the development of strong caller authentication and authorization mechanisms.<sup>34</sup> USTelecom agrees with this assessment, but such mechanisms – and possibly others – can more realistically be employed only once the transition to IP networks has been attained. This is the principal reason why our industry is actively engaged in the efforts of the Internet Engineering Task Force to develop a long-term technological solution in this area.<sup>35</sup>

Absent a meaningful transition to all-IP networks, stakeholders involved in this effort – consumers, industry and government – will be forced to deal with disparate technological measures deployed over two unique networks: IP networks that are capable of deploying more advanced technologies and solutions, and legacy TDM networks capable only of supporting more rudimentary technologies. This ‘TDM gap’ represents a drag on innovation for stakeholders focused on effectively addressing this issue.

---

<sup>34</sup> North American Numbering Council Meeting Transcript, September 18, 2013, p. 73 (available at: [ftp://ftp.fcc.gov/pub/Daily\\_Releases/Daily\\_Business/2014/db0327/DOC-326289A1.txt](ftp://ftp.fcc.gov/pub/Daily_Releases/Daily_Business/2014/db0327/DOC-326289A1.txt)) (visited January 16, 2015).

<sup>35</sup> The development of standards in this area for use in IP-based communications networks is the priority of the Secure Telephone Identity Revisited (STIR) Working Group activated in 2013 within the Internet Engineering Task Force (IETF). Such solutions will become most effective upon a widespread transition to IP-based communications networks, a process that is well under way. See e.g., Internet Engineering Task Force website, *Secure Telephone Identity Revisited* (available at: <https://datatracker.ietf.org/wg/stir/documents/>) (visited January 23, 2015).

## 2. The Challenge of Caller-ID Spoofing.

Another significant challenge that all stakeholders face in this area is what telephone number is delivered with each call – whether human or machine-initiated. Essentially the number that is delivered to the caller is the only information available to the end user to identify the purported calling party. Despite federal prohibitions, telephone numbers can be easily disguised, or deliberately spoofed at origination and through call delivery in a way that is malicious or fraudulent. Consumers may see a calling party’s number that they trust and answer the phone only to hear a pre-recorded message on the other end.

Despite the ease with which telephone numbers can be spoofed, some technologies deployed today rely heavily on the use of caller-ID information as the primary source of categorizing incoming calls as either legitimate or illegitimate. In general, these technologies function through the use of black lists and/or white lists.

USTelecom has previously discussed at length some of the technological limitations and potential risks to deploying services and tools heavily reliant on black list or white list technologies.<sup>36</sup> Because any phone number can be easily spoofed, technologies that rely extensively on the use of black lists can be easily circumvented. Although only a small universe of phone numbers is used by some bad actors to conduct their operations, others are increasingly randomizing the phone numbers that they employ in their calling schemes. Some are even using the phone number of the called party (or a close variation) when making calls.<sup>37</sup>

In the event systems relying on black lists are extensively deployed, bad actors can easily and rapidly transition to randomized numbers in order to circumvent such protections. In fact,

---

<sup>36</sup> *USTelecom Response*, pp. 6 – 11.

<sup>37</sup> See, USTelecom Press Release, *Caller ID Spoofing Scams on Increase: How Consumers Can Fight Back*, July 15, 2014 (available at: <http://www.ustelecom.org/news/press-release/caller-id-spoofing-scams-increase-how-consumers-can-fight-back>) (visited January 16, 2015).

the widespread deployment of a technology based on black lists could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify. This could increase instances of both “false positives” (*i.e.*, blocking numbers that should not have been blocked) and “false negatives” (*i.e.*, fail to block numbers that should have been blocked).

In this regard, the Commission asks the extent to which technologies produce false positives and/or false negatives. It is difficult if not impossible to accurately state what the actual rate or number of false negatives or false positives will be for particular services or devices. Despite the “paramount importance” of the ubiquity and reliability of the communications services,<sup>38</sup> the rate of false negatives or false positives could vary widely between services offered by different third-parties. This may particularly be the case where such services are overly reliant upon consumer-generated (*e.g.*, crowd-sourced) black lists that may be more prone to mistaken or – in instances of the spoofing of legitimate phone numbers – incorrect data entry.

Similarly, the Commission asks in its Notice whether it makes “a difference if the consumer is informed prior to purchase of the rate of false positives and false negatives, and therefore that legitimate or desired calls may be blocked.”<sup>39</sup> While this is a fair question for the Commission to consider, it is asked only from the perspective of the consumer *subscribing* to such a service (*i.e.*, the called party). An equally important concern for the Commission to consider is the potential impact of such services on *non-subscribing* consumers (*i.e.*, the calling party).

When innocent consumers’ phone numbers are spoofed and placed onto a black list, they will likely have no idea why their calls fail to complete, and they would be faced with a near-

---

<sup>38</sup> *Rural Call Completion Order*, ¶ 9.

<sup>39</sup> *Notice*, p. 3.

impossible task of figuring out how to fix the problem, or even who to contact. Serious legal and practical issues are also raised regarding a consumer's inability to have their legitimate calls completed for an undetermined period. Some companies offering black list services today have no mechanism in place to remove innocent, non-subscribing parties from their black list.<sup>40</sup> Even where an appeal process is available, it is disconcerting that an innocent impacted consumer would need to go through the time and inconvenience of such a process. It is entirely feasible that they could be unable to complete phone calls to their intended call recipients for days or perhaps longer, and this could raise serious health and safety issues. Legitimate businesses and public safety agencies could also be adversely affected due to their inability to place calls.

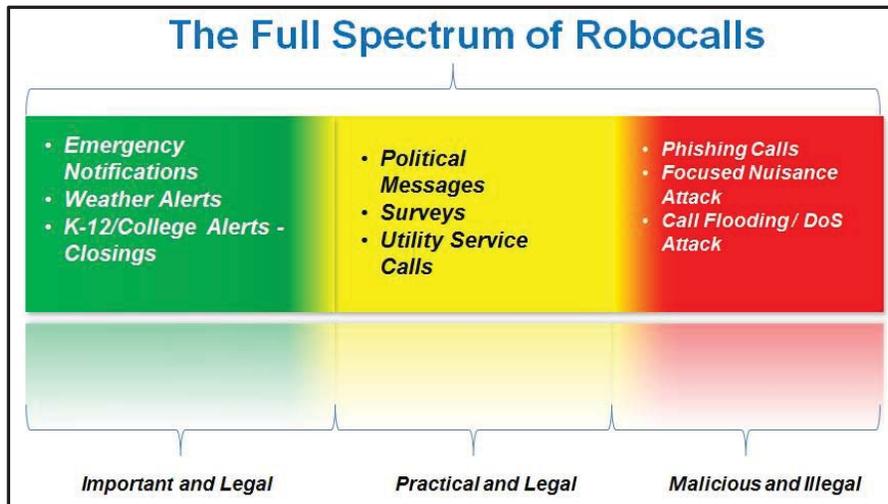
### **3. Carrier Limitations on Visibility Into Network Traffic.**

Carriers also have no visibility into the specific nature or type of call transiting their network, and therefore have no way of determining whether a specific call is illegal or legal. In addition to individual calls (*e.g.*, one consumer calling another), networks will also carry calls falling within the domain of the Do-Not-Call framework. As reflected in the below graphic, such calls can be analogous to a traffic light, falling into either the color green (*i.e.*, important and legal), yellow (*i.e.*, practical and legal) or red (*i.e.*, malicious and illegal).<sup>41</sup>

---

<sup>40</sup> Of the three services cited in the NAAG Letter (*i.e.*, Call Control by the Kedlin Company, NoMoRobo, and Primus Canada), none provides a mechanism for a non-subscribing consumer to have their phone number removed from their respective blacklists. For example, Call Control provides no information on its website regarding the removal of legitimate numbers from its black list. Although it provides a mechanism for anyone to submit information on an annoying or allegedly illegal calls, no similar portal exists for a consumer to have their legitimate number removed (*see*, Call Control website, Call Control & EveryCaller.com Support (available at: <http://www.everycaller.com/submit-call-report/>) (visited January 23, 2015). Similarly, while NoMoRobo's service offers a portal to its subscribers for reporting a valid number that was incorrectly blocked (*i.e.*, requiring a secure account and login), no similar mechanism exists for non-subscribing consumers to report blocking of their phone number by the service.

<sup>41</sup> In some instances, a particular call's location on this continuum is entirely dependent upon the geographic location in which the call is received. For example, some states have laws that



Given the instantaneous nature of voice communications, only the consumer receiving a call is in a position to see where on the spectrum a particular call resides. Conversely, service providers have no visibility into the specific nature or type of call transiting their network. Although providers can employ after-the-fact investigative techniques that can positively identify certain aspects of a call – such as whether it has been spoofed or not – there is no way for a carrier to make that determination in real time, as the call is transiting the network.

**III. Consumers Today Can Access an Expanding Assortment of Services From a Broad Range of Providers to Mitigate Do-Not-Call Abuses.**

In the face of these challenges, consumers today have access to a range of services designed to aid them in managing annoyances and harms, including those that may result from abuses of the Do-Not-Call framework. These services are available through a broad range of providers, including independent application developers, telecommunications carriers and equipment vendors. USTelecom shares the view of many other stakeholders that no single ‘silver bullet’ exists today that will comprehensively solve the problem.

---

regulate or prohibit political robocalls. Indiana and North Dakota prohibit automated political calls, while in New Hampshire, political robocalls are allowed, except when the recipient is in the National Do-Not-Call Registry.

Moreover, the involvement of multiple stakeholders in the deployment of various tools and technologies is calculated to yield favorable approaches for addressing this problem. As a result, the tools and technologies that ultimately prove worth pursuing will be better positioned to evolve and adapt to the changing robocall environment. A broad range of offerings and providers will also work to ensure that the unique needs of individual consumers are met, regardless of their underlying voice service or provider. This dynamic is crucial since the needs of any particular consumer will vary based on the network they are using (*i.e.*, wireline versus wireless), that network's underlying technology (*e.g.*, IP, TDM, Android, iOS, etc.), and even a consumer's level of technological savvy.

For example, the NAAG Letter highlights various tools deployed by independent application developers that are currently available to consumers. Among the services mentioned is "Call Control" for smart phones, developed by the Kedlin Company. Call Control is reliant upon a black list solution and can be deployed on wireless smart phones utilizing Android technology. Similarly, the NAAG Letter references 'NoMoRobo' – another black-list technology – that can be deployed over IP wireline networks supporting the simultaneous ring feature.

There are also offerings for consumers on TDM networks. Despite the presence of the previously discussed TDM gap, there are equipment developers that have deployed hardware for consumers who rely on such networks and seek to reduce or eliminate most robocalls. In general, these offerings complement existing Caller ID services by incorporating call blocking hardware in the consumer's customer premises equipment and home-communications set up. Depending on the equipment provider, such tools can utilize black lists, white lists or a combination of both. Similar to an answering machine, these devices usually connect between

the consumer's phone jack and their home telephone. Utilizing the caller ID service provided by their residential voice provider, the equipment passes through any calls appearing on the consumer's white list, and terminates calls residing on the black list. These devices generally range in price between \$40 and \$90.<sup>42</sup>

In addition to independent application developers, wireline and wireless companies have traditionally made a number of service features available to their customers to block unwanted calls. As is the case with services deployed by independent developers, the availability of tools provided by carriers will vary depending on the type of network over which those services are deployed.

For example, services such as caller-ID functionality and anonymous call-blocking are widely available over a variety of platforms.<sup>43</sup> Where carriers have deployed more advanced IP-based networks, consumers may also have access to more robust services. Some carriers offer a 'Do Not Disturb' feature that consumers can configure to control when they receive phone calls. Such services generally prevent some or all incoming calls from ringing on a customer's phone, and can be activated for a set period of time, or left on indefinitely. Consumers can either direct their incoming calls to a voice mailbox, or to an announcement stating that the person being called is not available. In addition, consumers can establish a list of phone numbers they will accept during these hours, which will bypass these safeguards, and allow the call to ring through.

---

<sup>42</sup> See e.g., Amazon.com website (available at: [http://www.amazon.com/s/?ie=UTF8&keywords=telephone+blocker&tag=googhydr-20&index=aps&hvadid=30015839247&hvpos=1t2&hvexid=&hvnetw=g&hvrnd=2264018295361446608&hvpone=&hvptwo=&hvqmt=b&hvdev=c&ref=pd\\_sl\\_2y9zynbyia\\_b](http://www.amazon.com/s/?ie=UTF8&keywords=telephone+blocker&tag=googhydr-20&index=aps&hvadid=30015839247&hvpos=1t2&hvexid=&hvnetw=g&hvrnd=2264018295361446608&hvpone=&hvptwo=&hvqmt=b&hvdev=c&ref=pd_sl_2y9zynbyia_b)) (visited January 23, 2015).

<sup>43</sup> Despite the prevalence of telephone number spoofing, consumers can still use caller-ID to ignore calls from phone numbers they do not recognize.

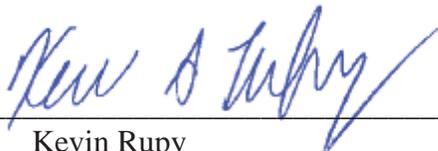
Because the offerings and capabilities of companies are different, consumers are always encouraged to contact their respective service provider in order to identify available resources.

**IV. Conclusion.**

USTelecom shares many of the same concerns raised by NAAG and others regarding abuses of the Do-Not-Call framework administered by the FTC. A host of complex technological and legal issues arise from the ongoing battle to address unwanted telemarketing calls; among them being the extent to which regulated common carriers can proactively and privately decide to block network traffic associated with the making and receiving of calls. Still, despite the technological challenges facing all stakeholders in this effort, consumers today can access a variety of services across differing voice platforms from a broad range of providers, including independent application developers, telecommunications carriers and equipment vendors.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: \_\_\_\_\_

Kevin Rupy  
B. Lynn Follansbee  
Jonathan Banks

Its Attorneys  
607 14th Street, NW, Suite 400  
Washington, D.C. 20005  
202-326-7300

January 23, 2015