

**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)	
)	

**REPLY 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

February 9, 2015

Table of Contents

I. Numerous Commenters Raised Concerns Over the Technological Limitations and Risks Associated with Broad Deployment of Blocking Technologies. 2

II. The Record Demonstrates That Diverse Offerings from a Multitude of Providers are Available in the Marketplace Across a Wide Variety of Platforms..... 9

III. The Commission Should Consider Expanded Outreach and Education to Consumers in Order to Increase Consumer Awareness and Empowerment on this Issue. 10

IV. There Is Consensus that All Stakeholders Should Drive Towards a Secure Caller ID Authentication Standard While Developing Better Interim Solutions..... 11

V. Conclusion. 12

* * *

Summary

The letter from the National Association of Attorneys General raises issues regarding the practical and technological challenges that may arise regarding the implementation of certain call-blocking technologies by common carriers to address the problem of robocalls. Many comments – including those from individual consumers – acknowledged USTelecom’s concerns regarding the technological limitations and potential risks to deploying services and tools heavily reliant on black list or white list technologies.

USTelecom and others discussed at great length the potential risks associated with broad implementation of black-lists, particularly as they relate to spoofing. For example, many commenters discussed concerns whereby innocent consumers could have their phone numbers spoofed by robocallers, resulting in their legitimate phone number ending up on a black list. The record clearly demonstrates that such concerns are not merely hypothetical.

Several commenters also expressed concerns regarding the conflation of “illegal” calls with “unwanted” calls. But as some commenters noted, it would be impossible to even make such a distinction since calls from certain organizations may be reported as unwelcome by some subscribers, while other subscribers may wish to receive them. There is an absence of any reassurance that the systems proposed would differentiate between legal and illegal. This is the primary reason carriers are cautious about deploying such technologies given their inherent risks, their inability to distinguish between “illegal” calls, “unwanted” calls and “legal” calls, and the lack of any Commission precedent directly addressing them, particularly with respect to the potential harms to calling or called parties.

The concern about overly broad blocking technologies interfering with legal calls was raised by various commenters. The record confirms that false positives do indeed occur, with one provider of blocking services acknowledging a “small number of false positives,” and another stating that “[f]alse positives and false negatives will undoubtedly occur.” But no party actually submits evidence supporting assertions that the various proposed blacklist based blocking solutions are “reliable.” USTelecom agrees that it is difficult if not impossible to accurately state what the actual number of false negatives or false positives will be for particular services or devices, but that does not justify the failure of proponents of specific blacklist-based solutions to share data about the potential for their services to cause negative externalities such as improper blacklisting of legitimate customers.

Although consumers benefit from competition among a diverse ecosystem of providers of robocall mitigation solutions, the Commission must still evaluate the important policy issues raised by the potential deployment by some competitors of over-broad blacklists. One of those policy concerns is the risk of externalities that can affect innocent legitimate customers who may not even know what a blacklist is.

The record in this proceeding affirms the view that 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 also agrees with numerous commenters who emphasized the important role consumer outreach and education can play in this area. Such outreach can substantially improve consumer understanding about the threats in this area, while raising awareness of the various industry and third-party tools that may be available to them. Public outreach measures have been successfully implemented by the federal government in the past and are ideally suited in the current context. USTelecom believes that dedicating more government resources to educating consumers about robocalls would go a long way toward ensuring consumers know what they should and should not do when they receive unwanted calls, and making them aware of the various options they have to protect themselves from such calls.

There is also consensus on the important work that is taking place across industry to address the problems of robocalls, caller ID spoofing and secure telephone number authentication. The Commission should support these various efforts including by identifying areas where additional research and developments may need to be emphasized. It should also, as advocated by USTelecom and others, facilitate the transition of the PSTN to an IP-enabled network. If the emergence of IP-enabled networks marked the start of the modern robocalling problem, the transition to a fully IP-enabled network will hasten solutions to that problem. The Commission should play a leadership role in supporting efforts to take advantage of the enhanced capabilities that IP networks have to detect and address robocalls.

* * *

**Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

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

**REPLY COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

The United States Telecom Association (USTelecom)¹ is pleased to submit its reply comments in the above-referenced proceedings.² In response to its Notice on the received from the National Association of Attorneys General (NAAG) letter (NAAG Letter),³ the Federal Communications Commission (Commission) received numerous comments from a broad range of stakeholders to include representatives from industry, consumer groups, carriers and individual consumers. Many of the comments filed with the Commission addressed issues and themes consistent with USTelecom’s initial comments in this proceeding.

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

² 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*).

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

I. Numerous Commenters Raised Concerns Over the Technological Limitations and Risks Associated with Broad Deployment of Blocking Technologies.

Many comments – including those from individual consumers – acknowledged USTelecom’s concerns regarding the technological limitations and potential risks to deploying services and tools heavily reliant on black list or white list technologies. The most notable technological challenges addressed in the initial comment round of this proceeding discussed the challenges and unintended consequences that could result from the broad implementation of black-list technologies.

USTelecom and others discussed at great length the potential risks associated with broad implementation of black-lists, particularly as they relate to spoofing.⁴ For example, many commenters discussed concerns whereby innocent consumers could have their phone numbers spoofed by robocallers, resulting in their legitimate phone number ending up on a black list.⁵ The record clearly demonstrates that such concerns are not merely hypothetical.

For example, one consumer commenting in this proceeding noted that robocalls she was receiving “show[ed] my neighbor’s name and telephone number; she is elderly and so I feel

⁴ See e.g., USTelecom Comments, pp. 11 – 17, ZipDX Comments, pp. 1 – 2, Trading Advantage Comments, p. 4, Verizon Comments, pp. 8 – 9, CTIA Comments, pp. 12 – 15, AT&T Comments, pp. 4. For a more detailed discussion of the various technological challenges associated with certain forms of call blocking see, USTelecom Detailed Response to Senator Claire McCaskill, pp. 6 – 11 (October 9, 2013) (available at: <http://www.mccaskill.senate.gov/imo/media/doc/RobocallDetailedResponsetoSen%20McCaskill.pdf>) (visited February 6, 2015).

⁵ See e.g., USTelecom Comments, pp. 16 – 17, ZipDX Comments, p. 1, CTIA Comments, pp. 12 – 15 (noting that at certain points, “numbers will appear in the blacklist that should not be blocked. These may include the numbers of political and charitable organizations . . . and the numbers of innocent subscribers whose numbers have simply been spoofed at random by robocallers.” CTIA Comments, p. 14), Trading Advantage Comments, pp. 4 – 5 (stating that “because Telephone Science and others like it are not required to disclose the algorithm they use to determine whether a call is a purported telemarketer, legitimate calls to consumers may be blocked with no recourse by either the consumer or the caller.”).

compelled to answer each time.”⁶ Yet another stated that he had been “tricked into answering a call from someone in my preferred list because the Robo caller was using [caller-IDs] from my home area codes.”⁷ Given the ease with which numbers can be spoofed, the broad deployment of black-list technologies would likely result in increased instances of such practices. As a result, innocent consumers’ numbers could be added to a black-list, resulting in their calling attempts being blocked.

In a related matter, several commenters expressed concerns regarding the conflation of “illegal” calls with “unwanted” calls.⁸ For example, the Marketing Research Association (MRA) notes that when the Commission asks about the effectiveness of different services in “blocking calls that consumers do not want,” it “mistakes an equivalency between unwanted calls and telemarketing calls.”⁹ It also emphasizes the absence of any “legal definition for calls that are simply unwanted,”¹⁰ and as CTIA points out, it would be impossible to even make such a distinction since “calls from certain organizations may be reported as unwelcome by some subscribers, while other subscribers may wish to receive them.”¹¹ MRA further notes the absence of any “reassurance that the systems proposed would differentiate between legal and

⁶ See, Comments of Patsy Carte, September 3, 2014.

⁷ See, Comments of Gerad Miller.

⁸ See e.g., Trading Advantage Comments, p. 4, Marketing Research Association Comments, pp. 4 – 5 (*MRA Comments*).

⁹ *MRA Comments*, p. 4.

¹⁰ *MRA Comments*, p. 4.

¹¹ CTIA Comments, p. 14. See also ZipDX Comments at 1 (“The desire of the consumer is to ‘block all robocalls’ or ‘block all illegal robocalls’ or ‘block all robocalls that I would find annoying’ or ‘block calls to my elderly parents when the call’s goal is to swindle them or sell them some needless, overpriced product.’ Agreeing to take on that request from a customer via call blocking will ultimately end in disappointment, and perhaps some dispute.”).

illegal.”¹² This concern is consistent with USTelecom’s discussion of this issue,¹³ and was also raised by other parties in this proceeding.¹⁴

While some of commenters cite various instances where carriers legally engage in various forms of call blocking,¹⁵ USTelecom agrees with AT&T that the examples cited “all share a common theme: they are consumer-directed.”¹⁶ But more importantly, the various blocking tools legally deployed by carriers have a very low risk of adverse or unintended consequences, since they generally deal with a discrete and verifiable universe of calls with little to no risk of adverse consequences.¹⁷

¹² *MRA Comments*, p. 4. Although Telephone Science Corporation (TSC) states that “the technology exists, today, to reliably and accurately detect illegal robocalls,” (*see*, Telephone Science Corporation Comments, p. 5), TSC offers no support for its implicit assertion that any particular technology can distinguish between lawful telemarketing or robocalls and unlawful telemarketing or robocalls.

¹³ *See*, USTelecom Comments, pp. 16 – 17 (discussing the lack of carrier visibility into the specific nature or type of calls transiting their networks, and an inability to determine whether a specific call is illegal or legal.).

¹⁴ *See*, Comments of Trading Advantage, p. 4 (noting that “without full inquiry into the methods by which Telephone Science determines whether a call is a probable telemarketer, the Commission cannot determine whether Telephone Science is blocking legal calls.”).

¹⁵ For example, various commenters cite instances of legal blocking by call carriers such as the blocking of 900 services, preventing consumers from making long distance calls for which a charge would be incurred, providing international call-blocking services to business customers and anonymous call rejection. *See e.g.*, FTC Comments, pp. 5 – 6, Global Tel*Link Comments, p 3.

¹⁶ AT&T Comments, p. 10.

¹⁷ For example, some of the instances cited by commenters – such as the blocking of calls to international or 900 numbers – only impact the calling party. Similarly, the provision of anonymous call rejection by carriers, also illustrates an instance where such calls are easily identifiable by both the carrier and the subscribing customer. Indeed, some of the services referenced by commenters as evidence of carriers engaging in call blocking were referenced by USTelecom and others in their initial comments in this proceeding. *See e.g.*, Comments of the Federal Trade Commission, p. 6 (citing as examples instances where carriers offer customers “Selective Call Rejection” (*80) to block calls from phone numbers on a customer-specified list; “Anonymous Call Rejection” (*77) to block calls that lack Caller ID identifying information;

USTelecom maintains that such services have a low risk of overreach (*e.g.*, instances of false positives), and unintended consequences.¹⁸ But this may not be the case with respect to the wide deployment of recently developed black list technologies that have been compiled by third parties from multiple sources, and that may not have been scrubbed to a degree of precision to minimize false positives and false negatives. This is the primary reason carriers are cautious about deploying such technologies given their inherent risks, their inability to distinguish between “illegal” calls, “unwanted” calls and “legal” calls, and the lack of any Commission precedent directly addressing them, particularly with respect to the potential harms to calling or called parties.¹⁹

The concern about overly broad blocking technologies interfering with legal calls was raised by various commenters. Global Tel*Link for example, stated that the Commission “must ensure that any authorized call-blocking technology does not sweep desired calls with unwanted ones.”²⁰ Contrary to the unsupported or implied assertions made by Telephone Science Corporation and others,²¹ such distinctions cannot currently be made based on the use of easily spoofable caller-ID information. As noted by Trading Advantage in its comments, “[w]ithout

and “Selective Call Acceptance” (*64) to block all calls except those from a specified list of phone numbers). *See*, USTelecom Comments, p. 9.

¹⁸ Of course, these solutions were developed before the current onslaught of unwanted Robocalls and have been criticized in the record as being ineffective as compared to other solutions. *See* Kedlin Comments at 3 (“offering consumers the ability to block 10-20 numbers is insignificant compared to the millions of spam calls placed daily, and offering consumers to block all calls but a predetermined list of callers significantly limits the functionality of their telephone.”); NUMBERCOP Comments, p. 4.

¹⁹ MRA asserts that there is “no demonstrable harm from survey, opinion and marketing research calls” and that such calls provide “significant benefit to consumers and the broader public” and that the coverage bias inherent in current call-blocking technologies could make users of such technologies “less likely to be represented” in the decennial Census. *MRA Comments*, p. 5.

²⁰ Global Tel*Link Comments, p. 4.

²¹ Telephone Science Corporation Comments, p. 5.

full inquiry into the methods by which Telephone Science determines whether a call is a probable telemarketer, the Commission cannot determine whether Telephone Science is blocking legal calls.”²²

Nor have proponents of third party-maintained blacklist solutions substantively engaged the Commission’s crucial question of “[t]o what extent do the technologies produce ‘false positives’ (*i.e.*, block numbers that should not have been blocked) or ‘false negatives’ (*i.e.*, fail to block numbers that should have been blocked)?”²³ The record confirms that false positives do indeed occur, with one provider of blocking services acknowledging a “small number of false positives,”²⁴ and another stating that “[f]alse positives and false negatives will undoubtedly occur.”²⁵ Another commenter describes its product as being developed to minimize false positives and negatives, has consumer controls to address those consequences, and ultimately concludes that “the end user acknowledges and accepts the risks of false detections by opting into a service.”²⁶ But no party actually submits evidence supporting assertions that the various proposed blacklist based blocking solutions are “reliable.”²⁷

²² Trading Advantage Comments, p. 4. Kedlin Company states that it has developed an algorithm that addresses the situation where a single caller ID of a “random, unsuspecting victim” will be “hijacked” and from which “thousands of outbound calls will be made from that number.” Kedlin’s proprietary product will monitor that activity and block calls originating from that caller ID until the calling party stops using the number and moves on to a different one, at which point the block is removed. Kedlin Comments, p. 4. Kedlin does not address how its proprietary solution would address thousands of outbound calls each with a unique spoofed Caller ID, randomly generated and assigned.

²³ Notice, p. 3.

²⁴ See, Comments of Telephone Science Corporation, p. 5.

²⁵ See, Comments of Numbercop, p. 5.

²⁶ Kedlin Comments, p. 4 (stating that such services should provide the means for identifying and accommodating false detections and provide the information transparently to the user).

²⁷ See, *e.g.*, Pindrop Security Comments, p. 1, Trading Advantage Comments, p. 2.

AT&T contends that while consumers should be made aware of the potential for false positives, ultimately, the rate of false positives is unknowable.²⁸ USTelecom agrees that it is difficult if not impossible to accurately state what the actual number of false negatives or false positives will be for particular services or devices,²⁹ but that does not justify the failure of proponents of specific blacklist-based solutions to share data about the potential for their services to cause negative externalities such as improper blacklisting of legitimate customers.

For example, one third party provider of a blacklist-based solution acknowledged a “small number” and false positives, but stated that “users are able to easily report them.”³⁰ It did not, however, provide data about how many complaints have been received from improperly blacklisted callers, or how long such callers were on the blacklist. Nor did it describe how it was “easy” for blacklisted customers to remove themselves from the list – which is important information for evaluating whether the “small number” of false positives of which the vendor is aware might actually understate the scope of the problem.³¹ Nor does it engage the scalability challenges that its blacklist solution will face if and to the extent it is deployed to a statistically relevant sample of subscribers. For example, it does not describe any techniques that it has developed to avoid unintended consequences such as the additional spoofing that may occur if and to the extent its service becomes deployed widely enough to create incentives for illegal robocallers to bypass it by more aggressive spoofing countermeasures.

²⁸ AT&T Comments, p. 13.

²⁹ USTelecom Comments, p. 15.

³⁰ Telephone Science Corporation Comments, p. 5.

³¹ Telephone Science Corporation does not appear to provide a portal for its subscribers to see any of the calls that have been blocked by its service. It is not clear how a consumer can “easily report” a missed call if he or she is not even able to determine it has been blocked.

While not specifically addressing the issue of false positives and false negatives, the FTC asserts that the current limitations and imperfections of call blocking technologies should not prevent consumers from having access to them, as long as providers of call-blocking services provide accurate disclosures to consumers when they sign up for these services that certain calls they want to receive may be blocked, because consumers should be able to “decide for themselves whether they risk the disruption of those calls.”³²

The FTC notes that “the market will address the issue” if a “call-blocking service blocks too many calls” because “call-blocking providers will either have to improve their technology or risk losing subscribers.”³³ Although consumers benefit from competition among a diverse ecosystem of providers of robocall mitigation solutions, the Commission must still evaluate the important policy issues raised by the potential deployment by some competitors of over-broad blacklists. One of those policy concerns is the risk of externalities that can affect innocent legitimate customers who may not even know what a blacklist is. Where large blacklists are compiled by unregulated, third-party solutions providers and subsequently “adopted” by consumers, the risk CTIA identifies is significant:

Such solutions can result in the delivery of unwanted calls or the blocking of calls that the consumer would have wanted to receive, and if deployed on a large scale could potentially affect the integrity of the PSTN because bad actors – in order to bypass blacklists – may initiate extensive use of “spoofing” techniques that could cause harm to all customers (including ones who never signed up for any blocking service).³⁴

³² FTC Comments, p. 7.

³³ *Id.*

³⁴ CTIA Comments, pp. 9 – 10.

II. The Record Demonstrates That Diverse Offerings from a Multitude of Providers are Available in the Marketplace Across a Wide Variety of Platforms.

The record in this proceeding affirms the view that 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.

The record demonstrates that consumers utilizing a wide variety of voice services can currently avail themselves of numerous tools and services to mitigate problems associated with robocalls. For example, CTIA discusses various tools available from carriers, smartphone manufacturers and application developers.³⁵ Various commenters also submitted information consistent with USTelecom’s filing demonstrating the availability of mitigation solutions for consumers.³⁶ AT&T, for example, submitted comments outlining the various tools available to its wireline, wireless, U-Verse and business customers,³⁷ as well as a survey of various third party products and services that it notes number in the “thousands.”³⁸ Although the Commission should be mindful of the limits and drawbacks of existing solutions, as well as their inability to scale in the current Caller ID spoofing environment, as a general matter consumers benefit when various stakeholders innovate and compete to provide meaningful defenses to unwanted robocalls.

³⁵ CTIA Comments, pp. 8 – 10.

³⁶ *See e.g.*, Comments of CTIA, pp. 8 – 10, AT&T Comments, pp. 5 – 7, Verizon Comments, pp. 5 – 7.

³⁷ AT&T Comments, Appendix A.

³⁸ AT&T Comments, Appendix B. AT&T’s comments also contain a detailed listing of complementary third-party initiatives focused on combatting illegal robocalls. *See*, AT&T Comments, Appendix C.

III. The Commission Should Consider Expanded Outreach and Education to Consumers in Order to Increase Consumer Awareness and Empowerment on this Issue.

USTelecom agrees with numerous commenters who emphasized the important role consumer outreach and education can play in this area.³⁹ Such outreach can substantially improve consumer understanding about the threats in this area, while raising awareness of the various industry and third-party tools that may be available to them. Public outreach measures have been successfully implemented by the federal government in the past and are ideally suited in the current context.

Both the Commission and the FTC have already done admirable work in the robocall arena, but further education could be focused on certain key areas. For example, in addition to its enforcement actions, the Commission consistently releases advisories ensuring compliance with the law and rules by senders of political prerecorded voice messages and autodialed calls.⁴⁰

The FTC also has published materials instructing consumers not to engage with robocallers, and conducted workshops focusing on this issue.⁴¹ But the record demonstrates that many consumers still do engage with such callers, not understanding that their actions (such as pressing ‘1’ to be removed from the list) will likely result in more robocalls.⁴² Similarly, despite

³⁹ See e.g., CTIA Comments, p. 15, Verizon Comments, pp. 7 – 8.

⁴⁰ See e.g., Enforcement Advisory, *Telephone Consumer Protection Act Robocall Rules, Warning Political Campaigns and Promoters Against Robocall Abuse*, DA 14-1505 (October 21, 2014).

⁴¹ See, FTC website, *How to Handle an Unexpected Sales Call* (available at: <http://www.consumer.ftc.gov/articles/0076-phone-scams#Protect>) (visited February 6, 2015); see also, FTC website, *Robocalls All the Rage: An FTC Summit* (available at: <http://www.ftc.gov/news-events/events-calendar/2012/10/robocalls-all-rage-ftc-summit>) (visited February 6, 2015).

⁴² See e.g., Comments of Ragis, filed January 22, 2015 (stating that “I finally answered and pressed 1 to let them know I was on the Do Not Call List and they should remove my number from their calling, assuming it was just telemarketing.”); Comments of Geraldine Bilyeu,

the legality of calls from politicians, charities and surveys, many consumers appear unaware that such calls are permitted.⁴³

USTelecom agrees that dedicating more government resources to educating consumers about robocalls “would go a long way toward ensuring consumers know what they should and should not do when they receive unwanted calls, and making them aware of the various options they have to protect themselves from such calls.”⁴⁴

Whether implemented on a broad public relations scale, or through targeted industry working groups, such outreach measures ensure that valuable information is disseminated and shared amongst target audiences. The FTC in particular has already conducted various forms of successful outreach in this area, including its 2012 workshop on robocalls, as well as the development of consumer-centric informational tools.

IV. There Is Consensus that All Stakeholders Should Drive Towards a Secure Caller ID Authentication Standard While Developing Better Interim Solutions.

USTelecom, CTIA, AT&T and Verizon have all outlined the important work that is taking place across industry to address the problems of robocalls, caller ID spoofing and secure

January 22, 2015 (stating that “Even when you have the option of talking to a human on the other end of the line, they disconnect if you ask them to please remove your phone number.”); Comments of Vicki Scherer, January 21, 2015 (stating that “I have tried staying on the line to talk to someone to ask them to removed my name from their call list only to be hung up on or talked rudely to.”).

⁴³ See e.g., Comments of Patricia Ryan, January 22, 2015 (stating that “I’m on the Do Not Call list, but that doesn’t seem to stop robo calls. The three most annoying are the Rachel from cardholder services, the IRS tax lawsuit, and all of the constant political calls during an election year.”); Comments of Chuck Strahm, January 21, 2015 (stating that “Please, please put an end to the practice of robotic phone calls for anything other than emergency purposes. It is so frustrating to have companies & politicians invade our privacy at any time that they choose.”); Comments of Pamela Kowalski, January 26, 2015 (stating that “I will receive from one to five calls a day for anything from “Windows tech support” to “Rachel at Card Services” (we have NO credit cards!) to colleges offering class information (I’m 65 yrs old!) to politicians, charities, consumer surveys, offers to have my carpets cleaned, furnace cleaned and windows replaced.”).

⁴⁴ Verizon Comments, p. 7.

telephone number authentication.⁴⁵ The Commission should support these various efforts including by identifying areas where additional research and developments may need to be emphasized. It should also, as advocated by USTelecom and others, facilitate the transition of the PSTN to an IP-enabled network.

The record is clear that as VoIP platforms emerged and personal computing technology advanced, the barriers to entry for unlawful robocallers dropped, the tools for Caller ID spoofing multiplied, and the mishmash of legacy TDM and emerging IP-enabled platforms enabled a literal international maze of networks that has facilitated the ability of call originators to disguise their origins and frustrate attempts by law enforcement. If the emergence of IP-enabled networks marked the start of the modern robocalling problem, the transition to a fully IP-enabled network will hasten solutions to that problem. The Commission should play a leadership role in supporting efforts to take advantage of the enhanced capabilities that IP networks have to detect and address robocalls.

V. Conclusion.

There is widespread agreement in this proceeding on the technological challenges and inherent risks associated with certain approaches to addressing violations of the Do-Not-Call framework. These concerns extend beyond the hypothetical, and the Commission should remain cognizant of the unintended consequences that could result from the broad implementation of black-list technologies.

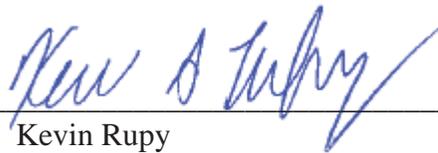
Despite these challenges, the record affirms the view that consumers today have access to a range of services designed to aid them in managing annoyances and harms, including those that may result from abuses of the Do-Not-Call framework. The Commission's should dedicate more

⁴⁵ See, AT&T Comments, p. 3, CTIA Comments, pp. 2 – 5, Verizon Comments, pp. 9 – 11.

resources towards educating consumers about robocalls, focusing on advising consumers of the tools available to them, and what to do when they receive unwanted calls. Finally, the Commission should support ongoing industry efforts to address the problems of robocalls, caller ID spoofing and secure telephone number authentication.

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

February 9, 2015