Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Robocalls and Call-Blocking Issues Raised By the National Association of Attorneys General	))))	CG Docket No. 02-278 WC Docket No. 07-135

To: The Commission

COMMENTS OF CTIA–THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

January 23, 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CTIA – The Wireless Association® ("CTIA") and its members supported the Telephone Consumer Protection Act's ("TCPA's") adoption in 1991, and have participated in the Federal Communications Commission's ("Commission's") implementation efforts since then. Wireless providers have worked with a wide range of standard-setting groups to combat unwanted calls, caller ID spoofing, and other forms of fraud. Industry members have been praised by the Federal Trade Commission for their cooperation with law enforcement authorities, conducted their own forensic investigations of unlawful activities, and brought suit against TCPA violators. This should be no surprise, for wireless carriers are themselves harmed by unlawful calling practice: Mass-calling events degrade and disrupt their provision of service, and customers frequently blame the providers themselves for unwanted calls.

In responding to the robocall problem, the Commission should exercise caution and work to avoid unintended consequences. Mobile providers, device manufacturers, and app developers already offer various tools that help consumers stop unwanted calls. For example, wireless providers have long offered customers access to vertical features that block calls from numbers selected by the customer, device manufacturers offer features such as "Do Not Disturb" and "Block Calls," and third-party apps enable customers to manage which calls they receive. These approaches, however, differ from the blocking solutions in which the National Association of Attorneys General ("NAAG") have expressed interest, which involve companies, rather than customers themselves, choosing which calls will and will not be completed.

Commission precedent clearly provides that Sections 201(b) and 202(a) prohibit voice carriers from blocking calls where customers have not asked them to do so. The Commission and the Wireline Competition Bureau have reiterated this principle multiple times since 2007, and the Enforcement Bureau has taken at least three significant enforcement actions based on a carrier's alleged failure to complete calls.

The wireless industry is open to clarification of the no-blocking rule as it relates to fraudulent activities, but any exception to the general no-blocking rule should account for the extensive options available from app providers today and for the unintended consequences that arise from use of the third-party blacklists. For example, even assuming an accurate database of blacklisted and whitelisted numbers can be compiled and maintained, the ease with which modern equipment and software can allow a caller to spoof a caller ID would present significant challenges. Moreover, the database for any blacklist would be very large and continually growing, such that maintaining and operating the database would be a massive undertaking. Even so, any third-party blacklist will necessarily include numbers it should not, and it can be very difficult for innocent parties to have their numbers removed. Likewise, the maintenance of third-party blacklists could raise significant customer privacy concerns.

The Commission does, however, have a role to play in stemming the tide of unwanted robocalls. Specifically, it can and should work to educate consumers about the causes of these calls and the various tools that they have at their disposal to prevent such calls on their own. This information could do much to mitigate robocall problems without risking the harms discussed above.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Robocalls and Call-Blocking Issues Raised By the National Association of Attorneys General	))))	CG Docket No. 02-278 WC Docket No. 07-135

To: The Commission

COMMENTS OF CTIA–THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® ("CTIA") is pleased to respond to the Consumer and Governmental Affairs Bureau's November 24 Public Notice addressing unwanted and unlawful automated "robocalls."[1] As described in detail below, CTIA and its members have long supported the Telephone Consumer Protection Act ("TCPA") and have played an active role in both the policy-making and law-enforcement processes that seek to protect consumers from unwelcome calls and messages. We applaud the efforts of the Commission, other governmental agencies, and third-party groups, and we look forward to working with policymakers to continue to protect consumers.

Telecommunications carriers have spent over a century designing networks to *complete* calls, and the prospect of blocking communications raises significant logistical and technical challenges. That said, carriers recognize the nuisance and real harms that unlawful robocalls cause, and have worked – along with device manufacturers and app developers – to provide tools consumers can use to manage the calls that ring on their phones. As described below, there are

[1] *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*, Public Notice, DA 14-1700 (Nov. 24, 2014) ("Public Notice").

significant legal and technical issues that the FCC should carefully consider as it reviews robocall mitigation practices.

I. THE WIRELESS INDUSTRY TAKES UNLAWFUL ROBOCALLS VERY SERIOUSLY AND HAS WORKED HARD TO PROTECT CONSUMERS FROM SUCH CALLS.

A. CTIA and Its Members Have Been Active Participants in the Policy-Making Process Regarding Unlawful Robocalls.

CTIA was proud to support initial adoption of the TCPA in 1991. CTIA, its members, and other members of the industry have remained active participants in related FCC dockets since that time. The FCC's first Report and Order implementing the TCPA in 1992 acknowledged participation from wireless providers and other communications industry members, including CTIA, AT&T, Ameritech, Bell Atlantic, Bell South, GTE, MCI, NTCA, NYNEX, Pacific Bell, Southern New England Telephone Company, Southwestern Bell, Sprint, U.S. West Communications, and The U.S. Telephone Association.[2] CTIA and its members also participated in the FCC's 2002 proceeding to revise the TCPA rules and implement the National Do-Not-Call List,[3] and remain active in various proceedings seeking clarifications of the Commission's TCPA rules.[4]

---

[2] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 7 FCC Rcd 8752, 8785-89 (1992) (Appendix A).

[3] The Report and Order notes that CTIA, AT&T Wireless, Cingular Wireless, Sprint, and Verizon Wireless participated in the proceeding. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014, 14166-73 (2003) (Appendix C). Other industry participants included BellSouth, Comcast, Cox, Intrado, NCTA, NTCA, Nextel, Qwest, SBC Communications, and Verizon. *Id.*

[4] *See, e.g.*, Comments of CTIA – The Wireless Association, filed in Petition for Expedited Declaratory Ruling of United Healthcare Services, Inc., CG Docket No. 02-278 (filed Mar. 10, 2014); Reply Comments of AT&T Inc., filed in Petition of 3G Collect Inc. and 3G Collect LLC for Expedited Declaratory Ruling that TCPA is Inapplicable to the Use of Automated Systems by Operator Service Providers Completing Collect Calls to Telephone Numbers Assigned to Cellular Telephones, Docket No. 02-278 (filed Dec. 10, 2012); Comments of CTIA – The

Industry members also have an extensive record of working to develop standards-based solutions to address the issues presented here in concert with a broad array of groups. For example, providers have worked with the Alliance for Telecommunications Industry Solutions ("ATIS") to develop standards and best practices to address the robocall problem.[5] ATIS has drafted rigorous guidelines and best practices that help network management personnel address traffic management issues that may arise during mass calling events.[6] ATIS helped public safety agencies optimize their deployment of Emergency Notification Systems to better ensure call completion without overwhelming affected networks. ATIS has also published reference information for responsible companies on the use of autodialers and on network security issues. Currently, ATIS is updating materials related to the deployment of next-generation networks in order to address concerns arising from mass calling events.[7]

Wireless Association, filed in Consumer & Governmental Affairs Bureau Seeks Comment on Petition for Expedited Clarification and Declaratory Ruling from Revolution Messaging, LLC, CG Docket No. 02-278 (filed Nov. 21, 2012); Comments of CTIA – The Wireless Association, filed in Consumer & Governmental Affairs Bureau Seeks Comment on Petition for Expedited Clarification and Declaratory Ruling from SoundBite Communications, Inc., CG Docket No. 02-278 (filed Apr. 30, 2012); Comments of Verizon and Verizon Wireless, filed in Consumer & Governmental Affairs Bureau Seeks Comment on Petition for Expedited Clarification and Declaratory Ruling from SoundBite Communications, Inc., CG Docket No. 02-278 (filed Apr. 30, 2012); Comments of Sprint Nextel Corporation, CG Docket No. 02-278 (filed May 21, 2010).

[5] Stopping Fraudulent Robocall Scams: Can More Be Done?, Before the Subcomm. On Consumer Protection, Product Safety, and Insurance of the S. Comm. On Commerce, Science, and Transportation, 113th Cong. 71 (2013) ("2013 Robocall Hearing") (Appendix, Response to written questions submitted by Hon. Claire McCaskill to Kevin G. Rupy) ("Rupy Hearing Response"), available at http://www.gpo.gov/fdsys/pkg/CHRG-113shrg85765/pdf/CHRG-113shrg85765.pdf.

[6] *Id.*

[7] *Id.* at 71-72.

Communications providers have also worked with the Internet Engineering Task Force ("IETF") to develop standards for secure call authentication. The IETF, which is the standards organization responsible for most VoIP standards, has formed an active Secure Telephone Identity Revisited ("STIR") Working Group, whose priority it is to develop standards for use in IP-based communications networks for authenticating callers.[8]

Likewise, through public-private partnerships such as the Communications Fraud Control Association ("CFCA"), industry stakeholders work alongside law enforcement to identify best practices and solutions to a broad range of telecommunications-related issues, including robocalls.[9] A collaborative public-private organization, the CFCA fosters critical relationships between individual industry stakeholders and law enforcement.[10] "These professional relationships are crucial to investigating and prosecuting individuals that engage in fraudulent activities occurring over communications networks, including illegal robocalls."[11] The CFCA also provides a forum for industry stakeholders and law enforcement to coordinate on issues relating to the latest scams, evolving investigations and cases, and other fraud-related matters.[12] This invaluable coordination helps public and private stakeholders stay ahead of the constantly evolving environment, and thereby more effectively combat the bad actors operating in this area.[13]

---

[8] Secure Telephone Identity Revisited (stir), IETF, http://datatracker.ietf.org/wg/stir/charter/ (last visited Jan. 13, 2015).

[9] Rupy Hearing Response at 72.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

Moreover, the Messaging, Malware and Mobile Anti-Abuse Working Group ("MAAWG"), which includes member companies from all over the world, targets ongoing and emerging messaging abuse issues.[14] MAAWG's Voice and Telephony Abuse Special Interest Group ("VTA SIG") works to mitigate abuse issues related to the convergence of the Internet and voice technologies – including robocalls – and focuses on education, best practices, end user reporting, feedback loops and collaborative solutions.[15] American MAAWG member companies include AT&T, Cablevision, CenturyLink, Comcast, Cox, Google, Sprint, Time Warner Cable, T-Mobile, and Verizon.[16] The VTA SIG is holding a workshop in February specifically addressing robocalls, caller-ID spoofing, and voice-phishing, which will focus on identifying key threats and actions to help reduce telephone services exploitation.[17]

B. Wireless Providers Have Actively Assisted Law Enforcement in Their Efforts to Eliminate Unlawful Robocalls.

The Federal Trade Commission has repeatedly acknowledged the wireless industry's assistance in combatting unlawful robocalls, and the industry has also conducted its own investigations and brought lawsuits under the TCPA. In 2009, for example, the FTC filed suit to stop illegal robocalls pushing vehicle warranty extensions. In a press release, the agency "acknowledge[d] the extraordinary cooperation that telecommunications carriers AT&T Mobility

[14] MAAWG (Jan. 23, 2015), https://www.maawg.org.

[15] MAAWG, Voice and Telephony Abuse SIG, https://www.maawg.org/vta-sig#About_VTASIG (last visited Jan. 23, 2015) ("MAAWG VTA SIG").

[16] MAAWG, Member Roster, https://www.maawg.org/about/roster (last visited Jan. 23, 2015).

[17] MAAWG VTA SIG.

and Verizon Wireless provided in the investigation of the case."[18] In 2010, the FTC again acknowledged the assistance that AT&T and Verizon Wireless provided when announcing a federal court injunction prohibiting a "[m]assive [r]obocall [o]peration."[19] And in 2011, the FTC highlighted the "invaluable" assistance it received from Verizon Wireless, AT&T, and CTIA in a case against a text spammer blasting text messages at a "mind-boggling rate."[20]

The industry also conducts its own investigations and brings lawsuits under the TCPA. In cases where CTIA's carrier members can locate and identify the source of illegal robocalls, the members have vigorously brought suit against the perpetrators.[21] Further, many companies maintain call fraud bureaus that will initiate investigations after a suspected mass calling event.[22]

---

[18] Press Release, Federal Trade Commission ("FTC"), *FTC Files Suit to Stop Illegal Robocalls Pushing Vehicle Warranty Extensions* (May 14, 2009), http://www.ftc.gov/news-events/press-releases/2009/05/ftc-files-suit-stop-illegal-robocalls-pushing-vehicle-warranty.

[19] Press Release, FTC, *At FTC's Request, Court Halts Massive Robocall Operation* (June 10, 2010), http://www.ftc.gov/news-events/press-releases/2010/06/ftcs-request-court-halts-massive-robocall-operation.

[20] Press Release, FTC, *FTC Asks Court to Shut Down Text Messaging Spammer* (Feb. 23, 2011), http://www.ftc.gov/news-events/press-releases/2011/02/ftc-asks-court-shut-down-text-messaging-spammer.

[21] 2013 Robocall Hearing at 39 (statement of Mike Altschul, General Counsel, CTIA – The Wireless Association) ("Altschul Statement"); Letter from Steve Largent, CEO, CTIA – The Wireless Association to Julius Genachowski, Chairman, FCC (Jan. 25, 2012) ("CTIA January 25th Letter"), http://www.ctia.org/docs/default-source/fcc-filings/ctia-sends-letter-to-fcc-regarding-tcpa-violations-associated-with-political-campaigns.pdf?Status=Master&sfvrsn=0. *See, e.g.*, Joshua Threadcraft, *Florida District Court Holds Whether Subscriber Or Person Who Answers Call Possesses TCPA Claim Depends On Circumstances*, JD Supra (Nov. 1, 2013), http://www.jdsupra.com/legalnews/florida-district-court-holds-whether-sub-23456/; Jane Musgrave, *Verizon Wireless sues South Florida companies, alleging customers getting thousands of illegal robocalls daily*, Palm Beach Post, Nov. 13, 2012, http://www.palmbeachpost.com/news/business/verizon-wireless-sues-south-florida-companies-alle/nS5kH/; Juan Carlos Rodriguez, Verizon, *OnStar Can't Use Consumer Law To Sue Over Robocalls*, Law 360 (May 8, 2012), http://www.law360.com/articles/338603/verizon-onstar-can-t-use-consumer-law-to-sue-over-robocalls.

[22] Rupy Hearing Response at 71.

Using traffic data forensics and other investigative tools, providers will try to identify the parties behind a particular mass calling event.[23] When they have been able to identify the entities behind these calls, companies often have sued the perpetrators and/or engaged law enforcement agencies and the Federal Trade Commission to investigate and prosecute illegal robocall incidents.[24]

C. Wireless Providers, Like Consumers, are Affected by Unlawful Calling Practices.

Wireless carriers have additional incentives to prevent unlawful robocalls as they are also impacted by unlawful calling practices. First and foremost, robocalls can adversely impact companies' networks.[25] Mass-calling events are highly localized, tremendously resource-intensive, and extremely brief – and providers receive no advance warning of these events. A severe mass-calling event can result in service degradation and disruption to phone services throughout a provider's affected area.

Second, carriers are impacted indirectly because they are unfairly blamed for calls and the Commission records TCPA complaints as complaints regarding wireless service.[26] Often, the first call a customer will make following a robocall is to the phone company. Customer service representatives must be trained to explain to customers the difference between legal and illegal robocalls, point them to the tools available to them to help mitigate these calls, and provide them

---

[23] *Id.*

[24] *Id.*

[25] 2013 Robocall Hearing at 32 (statement of Kevin Rupy, Senior Director, Law and Policy, United States Telecom Association) ("Rupy Hearing Statement").

[26] Altschul Statement at 38.

with information on how to file a complaint with the FTC.[27] Carriers must expend substantial resources to handle such customer inquiries and complaints.[28]

II. THE FCC SHOULD EXERCISE CAUTION TO AVOID UNINTENDED CONSEQUENCES.

A. Mobile Carriers, Device Manufacturers, and App Developers Already Offer Various Tools That Help Consumers Stop Unwanted Calls.

Mobile providers have long offered customers access to vertical features that block calls from numbers of the customer's choice, or that only permit calls from customer-specified numbers. These features help consumers prevent unwanted calls. Carriers typically offer a simple call-blocking capability that allows each customer to create a short "black list" of numbers from which he or she does not wish to receive calls,[29] as well as more sophisticated products that allow customers to identify specifically the numbers from which calls and messages may be delivered to devices in their plans, creating customer-generated black lists as well as "white lists" of permitted numbers, as desired.[30] Also, smartphone manufacturers provide various options, including "Do Not Disturb" and "Block Calls" features, that mobile

---

[27] Rupy Hearing Statement at 32.

[28] CTIA January 25th Letter at 1-2.

[29] *See, e.g.*, AT&T, *Block Calls and Messages to Your Wireless Phone*, http://www.att.com/esupport/article.jsp?sid=KB102428&cv=820#fbid=Ou756_WoCTu; Sprint, *Block, Restrict, or Allow Voice Calls Using MySprint*, (Nov. 5, 2014), http://support.sprint.com/support/article/block__restrict_or_allow_voice_calls_using_my_sprint/case-fk158645-20101105-114511; Video: Verizon, *How to Block Calls & Messages*, http://www.verizonwireless.com/support/how-to-block-calls-video/ (last visited Jan. 23, 2015).

[30] *See, e.g.*, AT&T, *Smart Limits, Your Family Smartphone Manager*, https://smartlimits.att.com/#/ (last visited Jan. 23, 2015); Sprint, *Parental Controls*, http://support.sprint.com/support/service/category/Parental_controls-Parental_controls (last visited Jan. 23, 2015); Verizon, *FamilyBase: How to Use*, http://www.verizonwireless.com/support/verizon-familybase-and-usage-controls/ (last visited Jan. 23, 2015).

customers can use to protect themselves.[31] Smartphone users already have access to a wide assortment of apps that – using blacklists, whitelists, and other techniques, permit consumers to sign up for whatever blocking (or other) solution they want. For example, Call Blocker is a free app that offers a range of features, including the ability to block unwanted calls.[32] Call Blocker can be configured to block all calls from numbers on a blacklist, all calls from non-contacts, or all calls from numbers that do not appear on a whitelist.[33] Similarly, the Truecaller app maintains a list of top spammers, allowing users to quickly block calls from all numbers reported as spam.[34]

These carrier-provided, smartphone-based, and third-party app-based capabilities are helpful in protecting consumers from unwanted calls and ensure, at minimum, that consumers do not receive more than a single unwanted call from a given number. These features are distinct from the blocking solutions in which the National Association of Attorneys General ("NAAG") has expressed interest, which involve companies, rather than customers themselves establishing lists of numbers from which calls are to be allowed or prohibited. 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

---

[31] *See, e.g.,* Apple, *Understanding Call and Message Blocking on iPhone, iPad, and iPod Touch* (Nov. 3, 2014), http://support.apple.com/en-us/HT201229; Kedlin Company Communication, *Call Control – Call Blocker* (Jan. 14, 2015) (available in the Google Play Android app marketplace), https://play.google.com/store/apps/details?id=com.flexaspect.android.everycallcontrol&hl=en.

[32] Jack Wallen, *Block unwanted calls on your Android phone with Call Blocker*, Tech Republic (Nov. 11, 2013), http://www.techrepublic.com/blog/smartphones/block-unwanted-calls-on-your-android-phone-with-call-blocker/.

[33] *See id.*

[34] Truecaller, http://www.truecaller.com/services/truecaller (last visited Jan. 23, 2015). Truecaller is available on both Android and Apple phones.

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).

B. The FCC Should Exercise Caution With Respect to Creating Any Exception to a Common Carrier's Obligation to Complete Calls.

The Public Notice seeks comment on how the Commission should respond to the NAAG's inquiries as to (*inter alia*) "[w]hat legal and/or regulatory prohibitions, if any, prevent telephone carriers from implementing call-blocking technology" and "upon what basis does the FCC claim that telephone carriers may not 'block, choke, reduce or restrict telecommunications traffic in any way."[35] Commission precedent on this issue is clear: As interpreted by the Commission, Sections 201(b) and 202(a) prohibit carriers providing a telecommunications service such as mobile voice from blocking calls where customers have not asked them to do so.

The Commission repeatedly has made clear that common carriers may not block, throttle, or otherwise impede calls. It found in 2007 that "no carriers … may block, choke, reduce or restrict traffic in any way" and that such conduct would constitute "an unjust and unreasonable practice under section 201(b) of the Act," because blocking "may degrade the reliability of the nation's telecommunications network."[36] In 2011, it reaffirmed these findings, and, extended the blocking prohibition to interconnected and one-way voice over Internet protocol ("VoIP") providers.[37] The next year, in the *Rural Call Completion* docket, the Wireline Competition

---

[35] Public Notice at 1-2.

[36] *Establishing Just and Reasonable Rates for Local Exchange Carriers*, Declaratory Ruling and Order, 22 FCC Rcd 11629, 11632 ¶¶ 5-6 (2007).

[37] *Connect America Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 18029 ¶ 974 (2011) ("*USF/ICC Transformation Order*"), *aff'd sub nom In re: FCC 11-161*, 753 F.3d 1015 (10th Cir. 2014).

Bureau reiterated that call blocking can be an unjust or unreasonable practice under section 201 of the Act, that selective call blocking can be an unjustly discriminatory practice under section 202, and that call blocking negatively affects the ubiquity and reliability of the telecommunications network.[38] And in the years since then, the Commission has taken enforcement action against three carriers alleged to have blocked calls. All three carriers entered into consent decrees with the Enforcement Bureau, agreeing to implement compliance plans to prevent call blocking and make voluntary contributions ranging from $875,000 to $2.5 million.[39] It is of course possible that, even now, the Enforcement Bureau is continuing to investigate additional allegations of call blocking by other carriers.

The wireless industry is open to clarification of the no-blocking rule as it relates to protecting against known fraud, or international revenue-sharing scams. But any exception to the general no-blocking rule as it applies to robocalls should account for the fact that consumers already have extensive blacklist-based options available from app providers and, as discussed below, blacklist solutions can have unintended consequences that impact all consumers. In any case, there is no need for mobile operators to begin implementing blacklist-based call blocking solutions, given the substantial number of apps that consumers can use to access third-party-options.

[38] *Developing a Unified Intercarrier Compensation Regime*, Declaratory Ruling, 27 FCC Rcd 1351, 1352 ¶ 4 (Wireline Comp. Bur. 2012).

[39] *Level 3 Comms., LLC*, Order, 28 FCC Rcd 2272 (Enf. Bur. 2013); *Windstream Corp.*, Order, 29 FCC Rcd 1646 (Enf. Bur. 2014); *Matrix Telecom, Inc.*, Order, 29 FCC Rcd 5709 (Enf. Bur. 2014).

C. Blocking Using Blacklists Raises Significant Logistical and Technical Challenges.

The NAAG Letter asks about a number of blocking solutions that have been developed by third parties. These technologies all rely on blacklists and whitelists generated through the collection of originating caller identification information about unwanted calls, as well as other information about caller identification for legitimate calls. Although these solutions offer superficial promise, there are technical and logistical problems that prevent them from being fully satisfactory to either consumers or policymakers. These include the following.

Caller ID Spoofing. Due to the ease of widespread caller ID spoofing, interconnected IP traffic can and does originate anywhere in the world, and neither the terminating carrier nor the customer can authenticate the sender. This is the most significant challenge for an approach based on blacklists and whitelists. Even assuming an accurate database of blacklisted and whitelisted numbers can be compiled and maintained, the ease with which modern equipment and software can allow a caller to hide his, her, or its identity by spoofing a caller ID would present significant challenges. It would, for example, be relatively simple for an illegal robocall generator to spoof one or more of the numbers on the whitelist to get its calls through the protection system. Similarly, robocallers could simply stop using an outbound number for caller ID purposes once it was placed on a blacklist. This concern is not at all hypothetical: Numerous commercial products are available that provide caller ID spoofing today.[40] In addition to products designed specifically for this purpose, cloud-enabled voice products (including both

[40] Examples include SpoofCard (Jan. 23, 2015), www.spoofcard.com; Bluff My Call (Jan. 23, 2015), www.bluffmycall.com; SpoofTel (Jan. 23, 2015), www.spooftel.com/freecall/; Caller ID Faker (Jan. 23, 2015), www.calleridfaker.com; TraceBust (Jan. 23, 2015), www.tracebust.com.

fixed VoIP services and mobile apps) include capabilities for caller ID spoofing.[41] The Truth in Caller ID Act prohibits spoofing of caller IDs for fraudulent or harmful purposes,[42] but unlawful robocallers willing to violate the TCPA are likely to be just as willing to violate another statute as well. This is particularly true for robocallers originating calls from outside the United States, who may be beyond the reach of U.S. law enforcement. The identification of illegal robocallers that are spoofing caller IDs is even more difficult if the robocaller routes VoIP calls through a proxy server; this makes them virtually impossible to trace.

Implementation and Scaling. Because unlawful robocallers typically use a large number of telephone numbers and change telephone numbers frequently, the database for any blacklist would be very large and continually growing, requiring a significant investment for both acquisition and maintenance of computer resources. Significantly, considerable capacity in both telecommunications and computer resources would be required to query the databases. In order for such a solution to work, the carrier would have to query the enormous blacklist and whitelist databases before delivering each and every call to every customer who used the service. At year-end 2013, U.S. wireless carriers handled over 218 *billion* voice minutes of use per *month*,[43] and millions of subscribers could be expected to sign up for call-blocking services. Maintaining and

[41] *See, e.g.*, Tristan Barnum, *How to Change or "Spoof" Your Caller ID With Voxox's Free iPhone App*, Voxox Blog (Jul. 18, 2013, 6:00 AM), http://blog.voxox.com/blog/bid/317811/How-to-Change-or-Spoof-Your-Caller-ID-With-Voxox-s-Free-iPhone-App.

[42] Truth in Caller ID Act of 2009, Pub. L. No. 111-331 (2010), codified at 47 U.S.C. § 227(e).

[43] CTIA, Annual Wireless Industry Survey, available at http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

operating the database would be a massive undertaking, and once deployed, the utility of this effort would be easily negated by the use of number spoofing. [44]

Accuracy/Reliability Issues. At certain points, numbers will appear in the blacklist that should not be blocked. These may include the numbers of political and charitable organizations, which may be reported by consumers because their calls are unwelcome even though not illegal (except when sent to wireless phones), and the numbers of innocent subscribers whose numbers have simply been spoofed at random by robocallers. Further, calls from certain organizations may be reported as unwelcome by some subscribers, while other subscribers may wish to receive them. Terminating carriers have no way to know when customers have opted in or otherwise consented to receive particular calls, nor could they be expected to know which numbers have been mistakenly added to a blacklist.

It does not appear that the existing call blocking solutions provide clear procedures for innocent people or organizations whose numbers have been placed on a blacklist in error (either through data entry errors or for one of the reasons discussed above) to have their numbers removed from the list. Such a procedure would need to be agreed upon and established before any system could be implemented. The Commission should be careful to avoid any "solution" under which the only remedy available to an innocent person is to obtain a new telephone number. At present, that is the only response to having one's number spoofed by a robocaller.

Privacy Issues. At least one reported robocall solution would require the carrier to allow the solution administrator to screen subscribers' incoming calls to determine whether they are from an unwanted robocaller, a permitted robocaller, or a live individual. Even if this kind of traffic screening is authorized by the recipient of the call, such a potentially invasive technology

[44] Recently, robocallers have begun spoofing the called party's own telephone number in the caller ID.

raises serious questions about consistency with the law and rules governing customer proprietary network information[45] and a carrier's traditional responsibility to avoid intercepting or divulging the content of communications other than in narrowly circumscribed instances.[46]

The continuing existence of all of these concerns militates strongly against an affirmative mandate for carriers to implement any particular call-blocking technology.

D. The Commission Should Expand Its Consumer Education Efforts With Respect to Call Spoofing, Robocalls, and Related Issues.

While mandates relating to the use of call-blocking solutions could have negative consequences and might even violate Title II' s no-blocking mandates, the Commission does have a role to play in stemming the tide of unwanted robocalls. Specifically, it can and should work to educate consumers about the causes of these calls and the various tools that they have at their disposal to prevent such calls on their own. To this end, the Commission could conduct outreach to inform customers about caller ID spoofing, the blocking capabilities already provided by many smart phones, and third-party solutions that are completely independent of the carrier's network. For example, many users of the Apple iPhone may not know that they can, through the "Settings" menu, chose to block calls from any numbers they like, or may use "Do Not Disturb" settings for temporary protection from calls. This information could do a great deal to mitigate robocall problems without risking the harms detailed above.

III. CONCLUSION

For the reasons discussed above, the Commission should make clear, to NAAG and others, that current laws preclude telecommunications carriers from implementing call-blocking solutions relying on third-party blacklists or whitelists, and that any mandate directing carriers to

[45] 47 C.F.R. §§ 64.2001 *et seq.*

[46] *See* 18 U.S.C. § 2510 *et seq*. (Electronic Communications Privacy Act).

implement such technologies would contradict the Communications Act and Commission precedent. The Commission should rely first and foremost on the market to promote development and implementation of robocall mitigation technologies.

Respectfully submitted,

By: */s/: Krista L. Witanowski*

Michael F. Altschul
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

January 23, 2015