BEFORE THE JOINT LEGISLATIVE PUBLIC HEARING ON THE 2020-21 EXECUTIVE BUDGET PROPOSAL: TOPIC PUBLIC PROTECTION

February 12, 2020

Albany, New York

Written Testimony of USTelecom – The Broadband Association in Opposition to S.7508-A.9508 (TED Article VII Budget Bill – Part T)

USTelecom appreciates the opportunity to submit written comments to the Joint Legislative Public Hearing on Public Protection. Our comments are focused on Part T of S.7508 and A.9508, titled "Robocalls".

USTelecom and its members, ranging from large global communications providers to small broadband companies and cooperatives, understand that our customers and your constituents are fed up with receiving illegal and unwanted robocalls. Illegal robocallers are abusing our networks and our customers and we are committed to doing everything possible to restore public trust in the phone system. Through USTelecom's nationally recognized Industry Traceback Group (ITG), we are working tirelessly to determine the source of these harassing calls and coordinating with providers and government to shut them down. USTelecom members are also empowering consumers with advanced call labeling and blocking solutions and deploying call authentication technology to prevent illegal caller ID spoofing. We do this because our customers deserve to be protected from illegal scammers, because it reduces the ability of fraudsters to achieve their objectives, and because it increases the confidence of consumers and businesses that rely on our networks.

There is no single solution or entity that can solve this problem. That's why we are focused on strengthening coordination with law enforcement authorities, including State Attorneys General and our federal partners at the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), the Department of Justice (DOJ) and other federal agencies. By helping law enforcement agencies quickly identify the source of illegal callers, together we can bring criminals to justice.

Together, industry and government – through enforcement and significant FCC and congressional policy actions – are actively collaborating at the national level to address this issue head on. USTelecom understands the interest of the Executive and the New York State Legislature to take action to protect its citizens, and there is an important role for the state in protecting consumers from illegal calls. However, we encourage the Executive and the New York State Legislature not to duplicate the active federal policymaking efforts in this space described below or, worse, adopt conflicting state rules and regulations.

Last summer, I was pleased to join the stage with three Attorneys General in Washington, D.C. to announce the adoption of anti-robocall principles by twelve national voice service providers along with every state Attorney General, including New York Attorney General Letitia James. The agreement adopted eight principles that these voice service providers, and hopefully others,

will implement to protect consumers and empower federal and state enforcement authorities to identify and prosecute bad actors. For example, the agreement includes a commitment from providers to "communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling" and to "dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group."[1] The principles also include a commitment to make call labeling and blocking solutions available to consumers and to authenticate calls to prevent caller ID spoofing. The agreement is a testament to the strong partnership between voice service providers and government enforcement authorities, and it reflects the most important role for the states in the fight against illegal robocalls – cracking down on criminals.

In addition to this state leadership, significant bipartisan efforts at the federal level are also being taken to prevent illegal and unwanted calls. For example, last June, the FCC approved new rules providing greater flexibility for voice service providers to block illegal and unwanted calls on behalf of their customers.[2] Also in June, building off of prior industry commitments to implement call authentication technology, the FCC proposed to require the adoption of such capabilities if major voice service providers fail to do so[3]. And in August, the FCC adopted new rules banning malicious caller ID spoofing of text messages and foreign robocalls.[4] These policy steps are in addition to the FCC's ongoing enforcement efforts.

The FTC is also an active cop on the beat, coordinating with the states and industry. In December, for the first time, the FTC joined with the Ohio Attorney General to shut down the operations of a VoIP provider responsible for enabling the origination of millions of illegal calls. And just this month the FTC announced that it put 19 additional VoIP providers on notice that they could be next. These actions built on enforcements taken last year. For example, in June, the agency announced a major crackdown on illegal robocalls, including 94 actions targeting operations around the country that are responsible for more than one billion calls.[5] And in January, the DOJ filed civil actions against two companies – one of which is located in New York – and individuals allegedly responsible for carrying hundreds of millions of fraudulent robocalls to American consumers. USTelecom's ITG assisted both the DOJ and FTC with these cases by providing critical data to track down the scammers behind these calls.

Preventing illegal and unwanted calls has also received bipartisan interest in Congress. In December, Congress approved S.151, the Pallone-Thune TRACED Act,[6] which was signed into

---

1 See Press Release, USTelecom, State Attorneys General Anti-Robocall Principles, (rel. Aug. 22, 2019) https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf.

2 *See Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 1951 (rel. June 7, 2019) (Call Blocking Declaratory Ruling & Third Further Notice).

3 *Id.*

4 FCC Bans Malicious Caller ID Spoofing of Text Messages & Foreign Robocalls, FCC (Aug. 01, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358841A1.pdf.

5 *See* Press Release, FTC, FTC Law Enforcement Partners Announce New Crackdown on Illegal Robocalls, (rel. June 25, 2019) *available at*, https://www.ftc.gov/news-events/press-releases/2019/06/ftc-law-enforcement-partners- announce-new-crackdown-illegal

6 Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S.151, 116th Cong.

law by the President in January. Among other things, the TRACED Act requires the FCC to mandate the implementation of call authentication technology, requires providers to provide free call blocking tools, increase penalties for illegal calls, and facilities stronger enforcement efforts. Related to tracebacks, the legislation requires the FCC to register a consortium of companies engaged in private-led efforts to trace back the origin of suspected unlawful robocalls and requires a report for voice service providers that have or have not participated in a private-led effort to trace back calls. Time is tight on these initiatives with the Act requiring implementation of some of these initiatives as early as next month and many additional steps will be taken by the FCC and other agencies this year as a result of the law.

In short, the FCC, FTC, DOJ and Congress – in partnership with industry – are actively engaged at the federal level in a multi-pronged effort to protect consumers and prevent illegal robocalls. These efforts provide a robust national framework to which voice service providers are subject. Combined with stepped up enforcement efforts by state Attorneys General, there has never been a greater focus on this critical consumer protection issue. It will truly take an all of the above approach to tackle this problem, and states can play an important role, particularly on the enforcement front. USTelecom has been pleased to closely coordinate with state Attorneys General on this issue. At the same time, USTelecom urges the state lawmakers not to adopt overlapping and potentially conflicting state requirements before allowing the important federal activities described above to take root. Nearly all illegal robocalls are generated using voice-over IP (VoIP) technology and are interstate, or often international, communications. It is thus extremely unlikely providers offering service in New York serve consumers across the country or region. The potential for a patchwork of competing state laws governing robocalls would be unnecessarily burdensome for providers and would also be confusing for consumers. As discussed above, states can and do play an important role in anti-robocall efforts, but given the very active effort at the national level, this is an area where duplicative or conflicting state laws is unnecessary and potentially harmful.

Industry Leadership

In addition to the federal regulatory and legislative activity summarized above, I would also like to highlight three areas of active industry leadership to address the illegal robocall epidemic.

- First, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as STIR/SHAKEN, that will substantially diminish the ability of illegal robocallers to spoof caller ID information. Companies of all types and sizes are deploying these standards into their IP networks today and will continue to do so throughout 2020. Once deployed, consumers will have more information about the identity of a caller or the type of call they are receiving. And carriers will be able to more accurately identify the source of calls, which will improve call traceback efforts.

- Second, more call labeling and blocking tools are available today than ever before to mitigate illegal or unwanted robocalls.

- Third, USTelecom's Industry Traceback Group is expanding its efforts to identify the source of illegal robocalls and working in close coordination with state and federal agencies

to assist in enforcement efforts. Recently, we have significantly enhanced our ability to trace back calls by automating the process. The time it now takes to trace back illegal robocalls has been reduced from weeks to days – sometimes even hours. Our average monthly traceback volume increased by 550% in 2019.

Industry is Committed to the Deployment of Call Authentication Standards

Industry is swiftly moving to implement the STIR/SHAKEN call authentication standard. Once implemented, the ability of illegal robocallers to spoof caller ID information will be significantly reduced and consumer knowledge about the validity of incoming calls will substantially increase. Numerous voice service providers – representing the wireline, wireless, and cable industries – have committed to deploying the SHAKEN and STIR standards within their respective networks. Deployment is active and ongoing.

While deployment of the SHAKEN and STIR standards is not a panacea to the robocall problem, these standards will improve the reliability of the nation's communications system by better identifying legitimate traffic. The deployment of the SHAKEN standard will also facilitate the ability of stakeholders (such as USTelecom's ITG) to identify illegal robocalls and the sources of untrustworthy communications.

Robocall Mitigation Tools are Increasingly Available to Consumers Across a Variety of Voice Platforms

Voice providers themselves and independent application developers are increasingly offering free services that can help New Yorkers reduce unknown and potentially fraudulent calls. Like efforts to authenticate calls, these tools alone will not solve the robocall problem, but they are an important tool that empowers consumers with the ability to better identify and/or block illegal or unwanted robocalls. Of course, the type of voice service a consumer purchases – whether it is wireless, wireline provided over VoIP technology, or wireline provided over the legacy Time Division Multiplexing (TDM) technology – will determine the types of tools available to customers.

Importantly, facilities-based providers are increasingly developing robocall mitigation tools themselves, and deploying them in their networks. For example, through its Spam Alerts service, for all wireline customers who have Caller ID (including ones served on legacy copper technology), Verizon provides enhanced warnings about calls that meet Verizon's spam criteria by showing the term "SPAM?" before a caller's name on the Caller ID display. The Spam Alerts feature proactively identifies and warns customers about potentially malicious robocalls. Verizon has also rolled out free spam alerting and call blocking tools to wireless customers whose smartphones support these features. Consumers can better decide if they want to answer a particular call, or they can choose to have spam calls sent straight to voicemail. In addition, AT&T's "Call Protect" service for customers with IP wireline phones, iPhones and HD Voice enabled Android handsets automatically blocks suspected fraudulent calls.[7] When activated,

[7] *See* AT&T, AT&T Mobile Security & Call Protect, *available at,* https://www.att.com/features/security-apps.html (last visited Feb. 11, 2020).

AT&T will automatically block fraudulent calls, warn of suspected spam calls, and allow consumers to block unwanted calls from a specific number.

Carriers, including USTelecom members CenturyLink, Windstream, Frontier, Consolidated and others, are also deploying a variety of additional tools across their TDM and IP networks, including "anonymous call rejection" services that block callers who intentionally mask their phone numbers and "no solicitation" services that make unidentified callers go through a screening step before ringing. Multiple providers that offer service over VoIP technology also work with Nomorobo to facilitate their customers' ability to use that third-party blocking service.

The multitude of blocking and labeling tools for different types of consumers reflects the fact that different types that technologies permit service providers to deploy different solutions. For example, whereas wireline customers on VoIP platforms and wireless customers have newer technologies that support consumer-facing opt-in blocking tools, the same types of tools are not supported by networks using the legacy TDM wireline technology.

Industry Traceback Efforts are Critical to Identifying the Source of Illegal Robocalls

Equally important for reducing illegal robocalls is the ability to identify the source of calls and a strong partnership between industry and government to share such information to go after bad actors. USTelecom leads the Industry Traceback Group,[8] whose members are committed to identifying the source of illegal robocalls and working with law enforcement to bring these illegal actors to justice.

There are over 30 members of the ITG, including traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies. The Communications Act permits voice providers to share customer proprietary network information (CPNI) in order to protect their customers and/or networks, enabling the ITG to quickly and efficiently identify the path of calls under investigation.[9]

Since late 2017, USTelecom has been making enforcement referrals to the FCC and the FTC based on the traceback results of the group. This industry/government partnership helps to streamline the enforcement efforts of both the FCC and the FTC, as well as states, who can now avoid the time-consuming process of issuing subpoenas to every provider in the call path. Instead, they can more efficiently focus their efforts only on those upstream providers that have declined to cooperate with the efforts of the ITG or who have refused to stop enabling illegal calls after they have been alerted that the calls they make possible are illegal.

---

[8] See The USTelecom Industry Traceback Group (ITG), What Is the Industry Traceback Group, *available at* https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/ (last visited February 11, 2020).

[9] Section 222(d)(2) of the Communications Act permits telecommunications carriers to share, disclose and/or permit access to, CPNI in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." 47 U.S.C. § 222(d)(2).

Given the crucial role of tracebacks in mitigating illegal robocalls, state lawmakers, the Executive and state authorities, consistent with the principles recently announced by Attorney General James, should strongly encourage voice providers to participate in traceback efforts.

* * * * *

There is no single solution to ending the scourge of robocalls, but progress is being made every day. USTelecom and our members are up to the challenge and are strongly committed to continue working together with government at all levels to substantially reduce, and ultimately eliminate, this problem. Thank you.