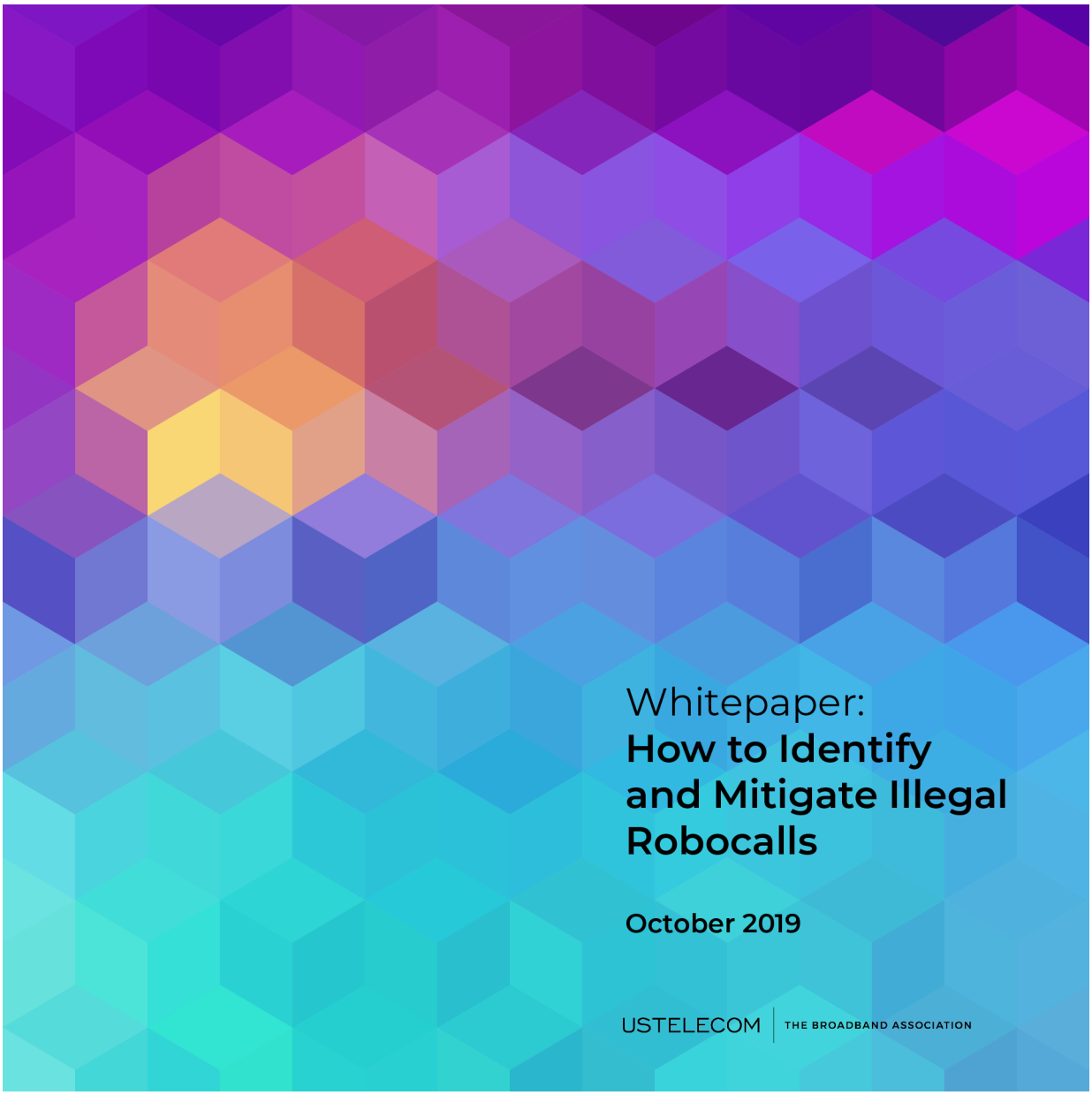
USTELECOM | THE BROADBAND ASSOCIATION



How to Identify and Mitigate Illegal Robocalls

By Farhan Chughtai

Contents

I. What is the Difference Between a Legal and Illegal Robocall? **3**

II. How Do Illegal Robocalls Get Onto, and Then Transit the Domestic Telephony Network? **5**

III. How Can Illegal Robocalls be Identified? **6**

IV. How Can Illegal Robocalls be Mitigated and/or Stopped in the Network? **7**

Citations **10**

USTELECOM | THE BROADBAND ASSOCIATION

How to Identify and Mitigate Illegal Robocalls

By Farhan Chughtai

USTelecom represents a diverse membership that ranges from large publicly traded global communications providers to small companies and cooperatives all of whom are committed to the security of the digital ecosystem as an essential driver of innovation, economic growth, public safety, our national security and other societal benefits.

We need solutions to the illegal robocall problem that will scale commensurate with the scourge. The plague affects hundreds of millions of telephone subscribers in the United States. But the bulk of the calls originate, on any given day, from a limited number of sources. First, this paper highlights what makes a robocall illegal. Second, it explains how an illegal robocall transmits through the telephony network. Third, it discusses how illegal robocalls can be identified by various technologies and the traceback processes. Finally, it provides a variety of mitigation techniques that can further reduce the illegal robocall problem.

I. What is the Difference Between a Legal and Illegal Robocall?

When assessing the robocall environment, it is important to make a distinction between legal and illegal robocalls. For example, federal law, such as the Telephone Consumer Protection Act ("TCPA"), does not prohibit any and all "robocalls"—a term that appears nowhere in the statute or the Federal Communications Commission's (FCC) rules. The TCPA regulates certain calls made using an "automatic telephone dialing system" or an "artificial or prerecorded voice" to residential and cellular phones, if a consumer has not consented to receive such calls.[1]

If a consumer has consented to receive a robocall, the call is legal. Legitimate businesses and organizations regularly utilize legal robocalls to provide consumers with critical and time-sensitive information, such as fraud alerts, school closures, prescription notices, and appointment reminders.

In contrast, the entities behind illegal robocalls regularly flout and ignore the federal and state laws governing the use of autodialers and prerecorded messages in order to indiscriminately call consumers. Such illegal robocalls can range from unlawful solicitations for products and services, to outright fraudulent and criminal activity (*e.g.*, calls purporting to be from the Internal Revenue Service that threaten arrest). Widely reported statistics on illegal robocalls sometimes artificially inflate call volumes by conflating legal and illegal calls.

While some of the federal rules governing the use of automated calls with prerecorded messages (*i.e.*, robocalls) are subject to interpretation, illegal robocalls can be identified where the calls in

question appear to violate one or more federal rules. The FCC and the Federal Trade Commission (FTC) implement and enforce various federal rules related to Caller ID spoofing, telemarketing practices, and calls made with an autodialer.

The **TCPA and FCC Rules**[2], enforced by the FCC, restrict certain calls made using an artificial or prerecorded voice to residential lines; certain calls made using an artificial or prerecorded voice or an automatic telephone dialing system to wireless telephone numbers; and certain telemarketing calls.[3]

The 2009 **Truth in Caller ID Act (TICIDA)**,[4] enforced by the FCC, includes a prohibition on the knowing transmission of misleading or inaccurate Caller ID information "with the intent to defraud, cause harm, or wrongfully obtain anything of value."

The **Do Not Call Implementation Act (DNCIA)**,[5] enforced by the FCC and FTC, authorizes the FTC to collect fees for the implementation and enforcement of a **Do Not Call Registry**. Telemarketers must consult the National Do Not Call Registry before calling.[6]

The **Telemarketing Consumer Fraud and Abuse Prevention Act (Telemarketing Act)** and **Telemarketing Sales Rule**,[7] enforced by the FTC, prohibits deceptive and abusive telemarketing acts or practices. The following is a list of a sampling of objective attributes that would make robocalls illegal when they are made without the express permission from the recipient:

- Calls made to mobile telephone subscribers using a pre-recorded or artificial voice.
- Pre-recorded or artificial voice calls that do not include the identification of the calling party at the beginning of the announcement.
- Pre-recorded or artificial voice calls that do not include the telephone number or address of the caller in the announcement.
- Calls with incorrect Caller ID information (when the calling number is not assigned to a party affiliated with the caller, as in the case of "neighbor spoofing").
- Sales calls to numbers on the Do-Not-Call list, where the calling party does not have a preexisting commercial relationship with the called party.
- Telemarketing calls that do not include an automated do-not-call option.
- Telemarketing messages left in voice-mail that do not include a toll-free call-back number that connects directly to an automated opt-out mechanism.
- Calls impersonating government officials.

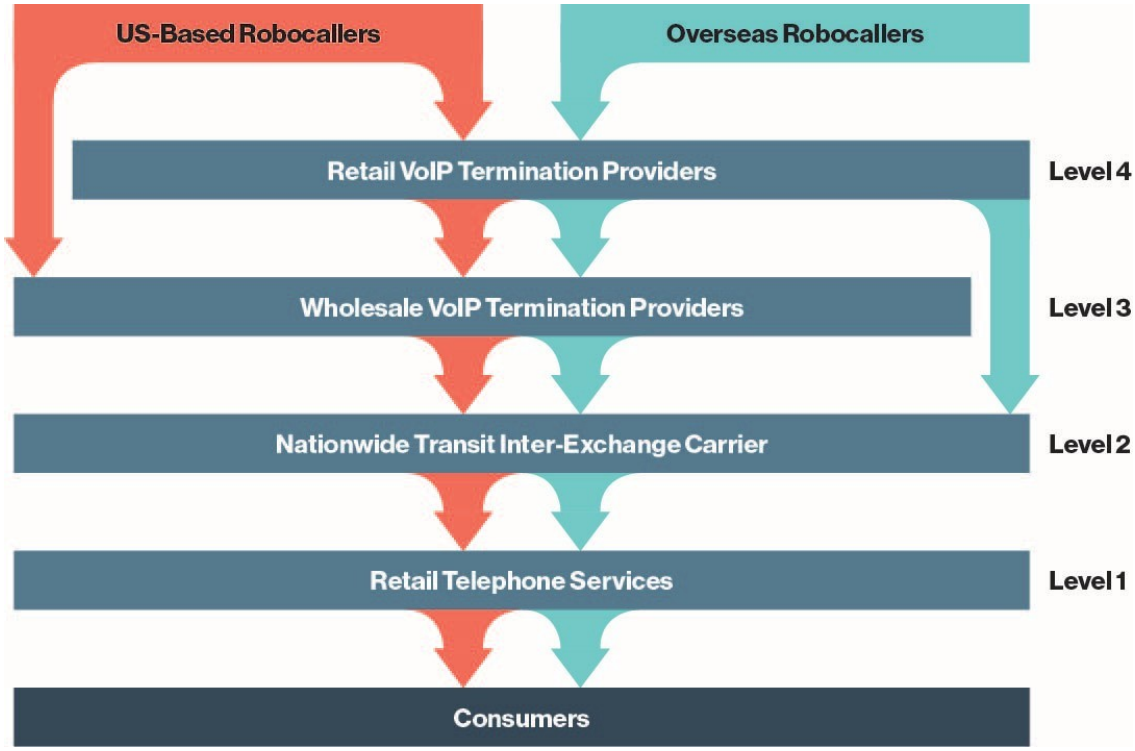
Note that when call examples include the audio content of a call (such as would be left on a consumer's voice-mail), some of the apparent violations can be more easily identified (*e.g.*, failing to include the identification of the calling party at the beginning of the announcement).

In addition to these robocall-specific statutes, certain illegal calls with the intent to commit fraud can also implicate additional fraud related statutes. Moreover, some individual states have their own laws and regulations that may apply.

II. How Do Illegal Robocalls Get Onto, and Then Transit the Domestic Telephony Network?

Before an illegal robocall can reach a consumer's phone, it must be originated by the caller and then transit a vast series of interconnected networks. Depending on from where the originating caller is located, their robocalls will transit a series of interconnected networks that are located domestically and – in some instances – internationally.

The diagram below shows the general path taken by illegal robocalls.



The robocaller, whether located in the United States or outside the country, buys "call termination" service from a US-based provider. This service, typically using Voice Over Internet Protocol (VoIP) allows robocallers to initiate calls and send them to the provider via the internet. (Levels 3 and/or 4)

Arrangements between the robocaller and originating provider may be structured on a "wholesale" or "retail" basis. Buyers of wholesale service often pay lower prices in exchange for higher volumes and are expected to resell the service to others. Generally, as we move down each level, the aggregate volumes increase and the per-minute prices go down.

The Level 3 or 4 provider that accepts the calls from the robocaller is designated the Originating Provider. That provider typically buys (via a wholesale arrangement) terminating service from yet another provider, and ultimately the calls are sent to a national transit provider (Level 2) who passes the calls to the providers directly serving the called consumers. These final providers (at Level 1) are the Terminating Providers.

I. How Can Illegal Robocalls be Identified?

Current network technologies do not enable a Terminating Provider to identify the Originating Provider. In fact, current network technologies only enable the Terminating Provider to identify the provider from whom it received the traffic. In addition, illegal robocallers can further evade their identification by changing the caller-ID associated with their calls (a practice known as "spoofing"). Fortunately, a new call authentication technology, known as SHAKEN/STIR, will change this dynamic.

SHAKEN/STIR is a framework of interconnected standards. SHAKEN/STIR are acronyms for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR) standards. Once implemented, calls traveling through interconnected phone networks will have their caller ID "signed" as being valid by originating voice service providers and verified by other voice service providers in the call path before ultimately reaching consumers. SHAKEN/STIR digitally validates the handoff of phone calls passing through this complex web of networks, allowing the voice service provider of the consumer receiving the call to verify that a call is from the person making it.

Once deployed by voice service providers, the SHAKEN/STIR standards will: 1) help to determine whether a caller-ID has been spoofed; and 2) identify the originating carrier behind the call. Although the SHAKEN/STIR standards do *not* determine whether a call is legal or illegal, the standards will greatly enhance the integrity of caller-ID and will help to more rapidly determine the true origin of a call.

Many large voice service providers are in the process of implementing this standard, but full nationwide implementation across all networks will take time.[8]

In addition to call authentication technology, equally important for reducing illegal robocalls is a process implemented by voice service providers to "traceback" the source of illegal calls. Traceback is an exercise where voice service providers who see malicious, fraudulent, illegal, spoofed and suspicious phone calls, seek information from ingress (upstream) Level 1 providers on who they received these suspicious phone calls from and going up-level until the Originating Provider is reached. In many cases the calling party information of suspicious phone calls is inappropriately being spoofed.

USTelecom leads the nationally recognized[9] Industry Traceback Group (ITG), a collaborative effort of numerous voice service providers from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls.[10] 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.[11] The ITG coordinates with voice service providers at all levels within the call path seeking to identify the source of, and eliminate, illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate.

Earlier this year, all 51 State Attorneys General and 12 national voice service providers announced their shared commitment to ending illegal robocalls, including a commitment to "allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group."[12]

An FTC action against an illegal robocall specifically acknowledged the assistance of USTelecom in bringing to justice an individual responsible for generating millions of illegal robocalls and calls to phone numbers listed on the Do Not Call Registry, including calls using "spoofed" caller ID information.[13] The FCC's Enforcement Bureau has sent letters to voice service providers that have been non-responsive to ITG traceback requests.[14] The letters "urge" voice service providers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls."

Given the crucial role of tracebacks in mitigating illegal robocalls, federal and state government enforcement agencies strongly encourage voice providers to participate in traceback efforts.

II. How Can Illegal Robocalls be Mitigated and/or Stopped in the Network?

The best place to stop illegal robocall traffic is where it first enters the telephony network through an Originating Provider. Moreover, since this is where the illegal robocall traffic is most concentrated, large volumes of traffic can be stopped before ever reaching consumers. As illegal robocalls move through the telephony network, the traffic becomes more dispersed (*i.e.*, spread across multiple Transit Providers) and is also comingled with other legitimate traffic. This dispersal and commingling of traffic can make detection and remediation efforts more difficult.

While much focus has been placed on blocking or labeling calls once they are delivered to the consumer's phone, such solutions often require the subscriber to download a smartphone app, and then enable and/or configure the service. In addition, most of these terminating-end solutions are technology-dependent and may not be available to all subscribers. Moreover, only those consumers utilizing such services will benefit from having some measure of protection.

These solutions are important. However, in contrast, mitigating and stopping illegal robocalls at the source benefits *all* consumers, regardless of whether they are utilizing a blocking service.

This more comprehensive and effective goal can be achieved by tracing back calls from illegal robocall campaigns, whereby the Originating Provider(s) can be identified, notified and directed to take steps to mitigate or stop the illegal robocalls.

Whereas SHAKEN/STIR only provides information on the Originating Provider, traceback identifies each of the voice service providers throughout the entire call path. As a result, if the Originating Provider fails to effectively address the illegal robocall traffic, the next downstream provider can be engaged to intervene.

There are a variety of mitigation techniques that network operators can utilize to mitigate or entirely prevent the transmission of illegal robocall traffic. An overview of these approaches is discussed below.

Know Your Customer: Voice service providers should confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of customer's business.[15]

This can help prevent Originating Providers allowing illegal calls from gaining access to Voice service providers' networks.

Monitor Network Traffic: Voice service providers should analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. This information can assist in the traceback process to identify the source of illegal calls.[16]

Require Traceback Cooperation in Contracts: Voice service providers should, for all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.[17]

Rejection by the Originating Provider: When an Originating Provider learns that their platform is being used as a conduit for illegal robocalls, they should identify the offending customer from the call examples provided by the relevant party (*e.g.*, call samples provided to them by the ITG), and then examine its call detail records (CDRs) for that particular customer. The Originating Provider should examine the CDRs for telltale signs of illegal robocall traffic, such as high call volumes, low duration calls, sequential dialing patterns, and call volumes to telephone numbers on the FTC's Do Not Call list. The provider may then impose network-level constraints, which can include throttling the rate at which the customer can initiate calls, restricting the number of concurrent calls, and limiting the caller-ID value(s) available for the customer's use. The provider may also decide that discontinuance of service is appropriate, especially if violations are on-going. New and existing overseas customers may warrant appropriate scrutiny before calls are allowed to be generated.

Intervention by the Next Level Provider: If the Originating Provider fails to mitigate the illegal calls or cooperate with contractual traceback commitments, downstream providers (which are receiving the calls from the Originating Provider) may want to consider whether they should continue to accept that provider's traffic. A downstream provider could notify an offending Originating Provider of terms-of-service and/or acceptable-use-policy violations, the terms of which generally prohibit the sending of illegal calls, and often have even more rigorous restrictions. If the traffic continues, the downstream provider could act according to the terms of its contract with the Originating Provider.

Government Enforcement Against the Robocaller: The FCC, the FTC, and State Attorneys General also have investigative authority to address crimes committed using illegal robocall technology. They often bring civil enforcement actions against a party placing illegal calls. This could then lead to additional criminal enforcement actions. Since the statutes generally specify

monetary forfeitures calculated on a per-call basis, penalties assessed on a single caller have grown in some instances to more than $100 million. The Department of Justice and other federal agencies also have investigative authority to address crimes committed using illegal robocall technology. Call records obtained from the Originating Provider could buttress these actions.

Enforcement Against Originating Provider: While government enforcers typically target the robocaller (end-user) initiating the illegal calls, the Originating Provider could also face potential legal exposure. Providers designated as "telecommunications service providers" enjoy certain protections from the actions of their customers, but also bear additional responsibilities with associated consequences. Under 47 U.S.C. § 201(b), the FCC can penalize telecommunications service providers whose practices it determines to be "unjust or unreasonable." Failure to take mitigating steps to stop illegal calls could satisfy the unjust and unreasonable criteria, especially in instances where high volumes of suspected illegal robocall traffic continue once the telecommunications service provider has been explicitly notified that they are a consistent conduit for such traffic. In addition to the FCC, State Attorneys General have various authorities; many Providers have state-specific registrations and licenses at risk. In addition to telecommunications-specific statutes, federal enforcement agencies and State Attorneys General could also pursue other types of violations including wire fraud and criminal conspiracy.

Conclusion

Stopping illegal robocalls at the source is the most effective way to quickly and comprehensively reduce the volume of illegal robocall traffic directed towards American consumers. Many of the tools necessary to achieve this goal, are available and are being pursued by government and industry stakeholders. These include frameworks for identifying illegal robocall traffic and measures and procedures to mitigate or prevent the origination of such traffic. Implementing such measures, however, requires active engagement and ongoing diligence on the part of all voice service providers in the United States, as well as cooperation and coordination with government stakeholders.

While implementation of such a framework involves great effort, it is the most effective way to prevent large volumes of illegal robocall traffic. There is no single solution to ending the scourge of illegal robocalls, but progress is being made every day.

[1] 47 U.S.C. § 227(b)(1)
[2] The TCPA is codified at 47 U.S.C. § 227. The Commission's implementing rules are codified at 47 CFR § 64.1200
[3] 47 U.S.C. § 227(b)(1)(A)-(B), (c); 47 CFR § 64.1200 (a)(1)-(3), (c)(2), (d)
[4] The Truth in Caller ID Act is codified at 47 U.S.C. § 227(e)
[5] The Do Not Call Implementation Act is codified at 15 U.S.C. § 6101
[6] Consumers may add their residential or personal wireless phone numbers to the National Do Not Call Registry to opt out of telemarking calls. As of October 1, 2003, it became illegal for most telemarketers or sellers to call a number listed on the National Do Not Call Registry. Federal Trade Commission, National Do Not Call Registry, *available at* https://www.donotcall.gov/faq/faqbusiness.aspx (last visited Oct. 16, 2019)
[7] The Telemarketing Act is codified at 15 U.S.C. §§ 6101-6108. The body of regulations adopted by the FTC to implement the Telemarketing Act is known as the Telemarketing Sales Rule. 16 CFR § 310
[8] Press Release, AT&T, AT&T, T-Mobile Deliver Cross-Network Call Authentication Technology (Aug. 14, 2019), *available at* https://about.att.com/story/2019/att_tmo_call-authentication.html (last visited Oct. 16, 2019); Press Release, Verizon, Verizon Offers New Ways to Battle Robocalls (Mar. 27, 2019), *available at* https://www.verizon.com/about/news/verizon-offers-new-ways-battle-robocalls (last visited Oct. 16, 2019); Press Release, AT&T, AT&T, Comcast Announce Anti-Robocalling Fraud Milestone Believed To Be Nation's First (Mar. 20, 2019), *available at* https://about.att.com/story/2019/anti_robocall.html (last visited Oct 16, 2019); Press Release, CenturyLink, CenturyLink and Neustar Team Up to Implement STIR/SHAKEN Call Authentication Solution and Help Restore Trust in Caller ID (Oct 16, 2019), *available at* http://news.centurylink.com/public-policy-blogs?item=855 (last visited Oct 16, 2019)
[9] *See* Remarks from Ajit Pai, Chairman, FCC, USTelecom Forum: Turning the Tide on Illegal Robocalls (June 11. 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-357911A1.pdf (FCC Chairman Pai publicly acknowledged the ITG, stating that "USTelecom has been particularly helpful in making sure that we can quickly trace scam robocalls to their originating source" and called USTelecom an "important ally in promoting broad industry participation" in traceback efforts)
[10] *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 Oct. 16, 2019)
[11] 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)
[12] *See* Anti-Robocall Principles, *available at* https://www.ustelecom.org/anti-robocall-principles/ (last visited Oct. 16, 2019)
[13] *See* Press Release, FTC, FTC Crackdown Stops Operations Responsible for Billions of Illegal Robocalls, *(*rel. March 26, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/03/ftc-crackdown-stops-operations-responsible-billions-illegal (last visited Oct. 16, 2019)
[14] *See*, Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Jonathan Spalter, President & CEO, USTelecom – The Broadband Association (Nov. 6, 2018), *available at* https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf (last visited Oct. 16, 2019)
[15] *See* Anti-Robocall Principles
[16] *Id*.
[17] *Id*.