Testimony of
Kevin Rupy
Vice President, Law and Policy
United States Telecom Association
before the
United States Senate Special Committee on Aging
"Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge"
July 16, 2014

Chairman Nelson, Ranking Member Collins, Members of the Committee, thank you for giving me the opportunity to appear before you today to present the current status and progress being made on the problem of phone scams. It is both timely and appropriate that the Committee take time to review this important consumer protection issue. The United States Telecom Association (USTelecom) and our member companies are aware of the problem associated with phone scams, which have been exacerbated by the new technologies enabling scammers easily and cheaply to initiate a large number of calls, also known as 'robocalls.' We understand the substantial harm these scams can cause to consumers, including seniors, and as a result we have long worked collectively and coordinated with relevant private and government stakeholders to address this issue.

My name is Kevin Rupy, and I serve as Vice President of Law and Policy at USTelecom. Our association represents innovative broadband companies ranging from some of the largest companies in the U.S. economy to some of the smallest cooperatives and family-owned telecom providers in rural America. Our members offer a wide range of communications services on both a fixed and mobile basis, and the overwhelming majority of them offer advanced broadband services including voice, video, and data. The customers that rely on our networks include consumers, businesses large and small, and government entities at the local, state, and federal levels.

This time last year, I had the opportunity to appear before the Senate Commerce Committee's Consumer Protection, Product Safety, and Insurance Subcommittee to discuss the burgeoning problem of robocalling. My testimony covered many issues that are relevant here: the impact of these calls on consumers and providers of voice services; the nature of these calls and why they have proliferated; the practical and legal challenges faced by our industry in addressing these calls; and steps our industry is taking to address this problem.

Today, I would like to inform the Committee of three important developments that have occurred in the last year. First, our industry has ramped up a concerted, broad-based, public-private effort focused exclusively on the issue of telephony abuse. Second, our member companies continue to work with government and industry stakeholders to develop more secure forms of caller identification authentication to more effectively address a practice that facilitates fraud, caller-ID spoofing. Finally, many of our member companies are offering services today that may substantially reduce the number of fraudulent calls.

Focused Industry and Government Initiatives

Our industry has initiated a focused effort within the existing framework of the Messaging, Malware and Mobile Anti-Abuse Working Group, or MAAWG, to address issues relating to telephony abuse. The MAAWG includes member companies from Asia, Europe, North America and South America that focus on a variety of initiatives to address ongoing and emerging messaging abuse issues.

Last year, the MAAWG formed the Voice and Telephony Abuse Special Interest Group whose sole focus is addressing the abuse occurring over telephone networks. The MAAWG created this working group to help protect telephony services from criminal activity and abuse by developing best practices, technologies and methods for mitigating phone-based attacks and scams. The working group is being led by co-chairs Alex Bobotek, of AT&T, and Dr. Mustaque Ahamad, professor at Georgia Tech's College of Computing. Participation in the working group includes representatives from the federal government (including the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), the Federal Bureau of Investigation, and the Department of Homeland Security) and industry, including USTelecom and several of its members.

This group engages in collaboration among government and industry stakeholders, outreach to standards bodies like the Internet Engineering Task Force (IETF), and writing Best Common Practices for carriers, consumers and all other links in the chain of communications. The group will also address various aspects of education in an effort to better protect and arm service providers, vendors, researchers, regulators and consumers with tools and information.

Since last July, the group has conducted two multi-day workshops for service providers, law enforcement, security vendors, academia, government and public policy officials, and other industry personnel interested in fighting telephony abuse. During these workshops, participating stakeholders received comprehensive briefings from recognized experts, collaborated on approaches for mitigating telephony abuse, and interfaced with industry and government counterparts. Another workshop is scheduled for early fall.

To enhance the results of this partnership, between these large industry meetings the group also organizes ad hoc teleconferences and targeted face-to-face events. As an active participant, I can attest to their value in enhancing our collaborative efforts to develop effective solutions to these issues.

Developing Standards to Battle Spoofing

In addition to the collaborative efforts of the MAAWG, our industry also continues to work within the IETF framework to develop technological standards for real-world solutions to address spoofing issues. Caller ID spoofing has become a common practice for scammers, since it is not yet possible to authenticate the identity of the callers behind traditional and Voice over Internet Protocol (VoIP) telephone numbers. But last summer, the IETF created a formal working group focused on creating a secure caller ID for IP-based communications. The IETF's "Secure Telephone Identity Revisited (STIR)" working group has been working since then to achieve this goal.

Despite the technological challenges, stakeholders within the IETF share the view that a cryptographic approach for VoIP can provide a much stronger and less spoofable assurance of identity than the legacy telephone network provides today. These stakeholders include representatives from industry (including many USTelecom members) as well as government (including the FCC's Chief Technologist). As evidenced by our member companies' participation in this effort, the standards to be developed by the IETF STIR working group have the full support of our industry.

Since commencing its efforts, the IETF STIR has made important progress. In May of this year, the group identified new strategies for attaching a secure identity to VoIP phone calls, and developed high-level requirements for solutions in this space. Earlier this month, the working group released a document that outlines a mechanism for securely identifying originators of VoIP telephone calls. While these efforts remain a work in progress, it continues to press forward to develop this important technological standard.

Such solutions will become most effective upon a full transition to IP-based communications networks, a process that is well underway. Public policies that foster investment in broadband and encourage the complete transition to IP-based voice services will hasten the day when the industry will have the kinds of tools it needs to attack illegitimate robocalling and caller ID spoofing.

Powerful Tools Available to Seniors Today

Finally, I want to use this opportunity to emphasize once again that our members are providing – and will continue to develop – various services that consumers can use to help mitigate the robocall problem. Because the offerings and capabilities of companies are different, consumers are always encouraged to contact their respective service provider in order to identify available resources. However, I would like to highlight just some of the services that are currently available to many consumers from our member companies.

Consumers subscribing to Verizon FiOS Digital Voice service can utilize the company's 'Do Not Disturb' feature. The service prevents some or all incoming calls from ringing on a customer's phone, and can be activated for a set period of time, or left on indefinitely.

Consumers can either direct their incoming calls to a voice mailbox, or to an announcement stating that the person being called is not available. In addition, consumers can establish an "Accepted Callers List" for up to ten numbers that will bypass these safeguards, and allow the call to ring through. The service can be accessed by the consumer through a convenient online manager that enables them to monitor and update their calling preferences. So, for example, using this FiOS Digital Voice service, a consumer can add or delete phone numbers to their Accepted Callers List, or change the period of time for which the service is activated.

A similar service known as "No Solicitation" is also available through CenturyLink. Once the No Solicitation service is activated, incoming calls are screened from 8:00 a.m. to 9:00 p.m. every day. An automatic message asks solicitors to hang up, and tells regular callers to press 1 to complete the call. Like the FiOS Digital Voice offering, consumers can also set up a privileged list of accepted callers who will automatically bypass the solicitor screening. This privileged caller list allows up to 25 entries, which can be entered by using either an area code (thus, allowing all calls from the identified area code), area code and prefix (allowing calls from the local exchange), or specific ten-digit telephone numbers. In addition, frequent callers are automatically added to the list. To be automatically added, a caller with a valid 10-digit number must call and press 1 at the No Solicitation message five times within seven days. AT&T offers a similar call screening service through its U-verse voice service product. That service can be activated to allow a customer to accept calls from up to 20 designated numbers, while directing any remaining calls to a standard message.

These are just a few examples of services that are available to many consumers today that can substantially lessen the ability of scammers to prey upon our nation's seniors. Whether a senior citizen activates these services on their own, or through the assistance of a family member, these services heighten the certainty that calls being received are coming from someone they know.

The availability of these and other tools may vary by service provider and location. Where these features are not available, consumers should work with their respective service provider to identify other tools that may be of assistance. For example, despite the prevalence of telephone number spoofing, consumers can still use caller-ID to ignore calls from phone numbers they do not recognize. Moreover, there are other third-party services in the marketplace today that can either complement or supplant services offered by our member companies.

Robocalls are a Problem for Consumers and Providers of Voice Services

USTelecom's member companies are all too aware of the increasing consumer frustration attributable to robocalls. Probably all of us in this room have experienced such calls. They are intrusive and disruptive. That's bad enough. But through some calls' deceptive pitching of phony products and services such as debt reduction programs and mortgage modification scams, the criminals behind these calls are stealing money from unsuspecting consumers.

Oftentimes, these scams are directly targeted towards senior citizens. This past March, the FTC moved to close down a multi-million dollar telemarketing fraud that targeted U.S. seniors across the nation, scamming tens of thousands of consumers.

In addition to the harm they cause to consumers, robocalls adversely impact USTelecom's own member companies. Often, the first call a consumer will make following a deceptive robocall incident is to their phone company. Our member companies' customer service representatives represent the first line of defense on this issue, and must be well versed in explaining to customers the difference between legal and illegal robocalls, pointing them to tools available to help them mitigate these calls and providing them with information on how to file a complaint with the FTC.

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

What Are Robocalls and Why Have They Proliferated?

The proliferation of robocalls has resulted from three major changes in the communications marketplace. The global reach of the Internet, combined with the widespread availability of mass-calling technology and a dramatic reduction in the costs of long-distance service, have radically changed the capabilities and economics of robocalling. As former FTC Chairman Jon Leibowitz observed, the Internet has allowed "voice blasting technology to flourish at bargain basement prices."

Looked at through the lens of history, we can sympathize with the frustration you must feel at the apparent growth of this problem over the last two decades in spite of repeated legislative efforts to put an end to it. Those efforts illustrate the difficulty of keeping the law ahead of the law-breakers – and ahead of technology. The FTC was specifically directed under the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 to adopt rules prohibiting deceptive and abusive telemarketing acts or practices, including "unsolicited telephone calls which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy." The body of regulations adopted by the FTC to implement this 1994 Act is known as the Telemarketing Sales Rule. The FTC is also empowered generally to address unfair or deceptive acts or practices in or affecting commerce, which the Federal Trade Commission Act declares unlawful. But the FTC's jurisdiction does not extend to common carriers, which are subject to the regulatory authority of the FCC. And for reasons described below pertaining to both our common carrier and privacy obligations, our member companies must complete phone calls.

Viewed from the perspective of communications law, when Congress adopted the Telephone Consumer Protection Act of 1991 (TCPA) to address telemarketing robocalls, its major purposes were to protect the privacy and public safety interests of telephone subscribers by placing restrictions on automatic dialers, fax machines, and unsolicited automated calls. The TCPA amended Title II of the Communications Act of 1934 to add a new section 227, entitled "Restrictions on the Use of Telephone Equipment." The nature of the technology being used in 1991 is well-illustrated by a consumer complaint listed among several examples in this Committee's report accompanying the bill (S. Rept. 102-178): "the automated calls filled the entire tape of an answering machine, preventing other callers from leaving messages." Except for amendments to expand the reach of section 227 to offshore callers and to prohibit caller-ID spoofing, the robocall provisions of the law remain largely as they were enacted in 1991 – and, as we all know, they have become increasingly ineffective.

The explanation for this is, regrettably, fairly simple. The original phone network was a "closed" system, meaning that voice services were generally provided by local exchange carriers and long distance companies through only the public switched telephone network (PSTN). These companies were providing what is called "plain old telephone service," or POTS. When Congress passed the TCPA in 1991 to address robocalls, autodialing systems, and certain fax machine problems, and even when it acted again three years later to deal with unsolicited telemarketing calls, wireless communication was only beginning to emerge and even dial-up Internet access was not yet a reality for mass consumer use. In contrast to the situation that confronted Congress in the early 1990s, today's communications services are provided not by the historical closed PSTN but by a "network of networks."*

As a result, voice service is now available from a myriad of companies with a diverse technical heritage. We still have the PSTN, but we also have VoIP providers, Internet service providers, and cable companies offering "phone" service, right alongside competitive local exchange carriers and wireless carriers. Approximately 40% of U.S. households have "cut the cord" and rely entirely on wireless for their voice service. And by the end of 2014, USTelecom estimates that between 55% - 60% of wireline households will subscribe to interconnected VoIP, oftentimes provided by the local cable company. Finally, "over-the-top" VoIP services – which use existing broadband networks – are widely available to American consumers and are offered

* To put this in further perspective, the first website was created in 1991 – the year of the TCPA's enactment. Today, there are more than 30 trillion individual web pages.

by some of the country's most prominent companies, including Vonage, Google Voice, and Microsoft's Skype service. Skype, for example, disclosed to the Securities and Exchange Commission in August 2010 that the company had 20 million connected users in the United States, 1.9 million of whom were paying customers.

Regardless of their delivery platform, each of these voice providers must ultimately connect to the PSTN because the reliability of their service to their own customers depends on their ability to deliver any call to anywhere. As a result, "phone" calls can connect to anyone, anywhere, regardless of whether a consumer's phone is connected to the PSTN, or their wireline or wireless phone or computer is connected to a broadband network. But this same remarkable connectivity – a connectivity we celebrate and want to expand to those Americans who don't yet enjoy it – also makes it possible for robocalling con artists and fraudsters to set up shop virtually anywhere in the country or even the world and, with the right equipment and a few clicks of the mouse, begin auto-dialing unsuspecting and vulnerable consumers across the United States.

The Contextual Nature of Robocalls – What the Consumer Sees

Now that we understand the network framework under which robocalls operate, it is important to understand the various types of robocalls. It can be helpful to consider all mass calling and robocall events as a traffic signal, comprised of green, yellow, and red lights. Robocalls that are important and legal would fall into the "green" category; robocalls that are legal, but whose usefulness are a matter of subjective personal opinion, would fall into the "yellow" category; and malicious and illegal robocalls would fall into the "red" category.

So, for example, a consumer may receive a “green” robocall from his or her child’s school, stating that the school’s opening will be delayed due to bad weather. Similarly, public safety agencies will often use robocalls to provide critical public safety messages. For example, Los Angeles County has implemented an emergency mass notification system used by the County’s Emergency Operations Center to notify residents and businesses of emergencies or critical situations and provide information regarding necessary actions, such as evacuations due to wildfires. Because the system uses geomapping, emergency notifications can be directed to very specific geographic areas. Clearly, robocalls of this type would fall into the “green” category.

Robocalls falling on the “yellow” spectrum are also legal, although some recipients might be indifferent to their messages or might prefer not to receive them. A doctor’s office may use a robocall to remind a patient of an upcoming appointment. Similarly, political candidates and political groups will often use robocalls to solicit votes in an upcoming election, or to deliver an advocacy message.

Finally, there are the instances of illegal calls falling into the “red” category of calling events. These calls include the infamous “Rachel from Card Services,” as well as other bogus schemes selling everything from cruises to insurance. Robocallers are becoming increasingly creative in perpetrating their scams, many of which originate from beyond our nation’s borders.

The traffic from a robocaller directed toward a consumer on the PSTN can transit the network either over the Internet, or through the PSTN itself. In fact, it is usually the case that a typical mass-calling event will transit multiple networks – encompassing both the PSTN and the Internet – before finally reaching the consumer.

The Contextual Nature of Robocalls – What the Service Provider Sees

Consumers are the only ones who can ultimately determine the nature of any specific robocall. Service providers, conversely, have no visibility into the specific nature or type of robocall transiting their network. They have no way of determining whether the call is illegal or legal. The service provider may only see that a mass calling event is taking place at a specific point on their network.

From the service provider's perspective, these mass calling events are defined by four characteristics. First, they are highly localized in nature. Second, they are represented by a high volume of calls. Third, once the calls arrive at their intended local target, they are extremely brief – potentially only lasting a matter of seconds or minutes. Finally, there is no advance warning for these calls.

Adding further complexity to the robocall issue is the problem of caller-ID spoofing – misrepresenting one's identity using a deceptive caller-ID. Although, after the fact, providers have investigative techniques that can positively identify whether a call has been spoofed or not, there is no way for a carrier to make that determination in real time, as the call is transiting the network.

Significant Legal Constraints Limit Potential Robocall Deterrents

Two primary legal issues face USTelecom's member companies with respect to remedying the robocall problem. First, under existing laws to which USTelecom's members are subject for their provision of legacy voice service, phone companies have a legal obligation to complete phone calls. These companies may not block or otherwise prevent phone calls from transiting their networks or completing such calls. The current legal framework simply does not allow our companies to decide for the consumer which calls should be allowed to go through and which should be blocked.

Second, there are substantial privacy issues that arise in any discussion relating to proposed robocall solutions. Robocalls are extremely contextual in nature. Depending on the nature of the call, certain robocalls are permitted under the law, while others are prohibited. Proposed solutions to the robocall dilemma that seek to make phone service providers the arbiter of whether a call should – or should not – be permitted to proceed skirt dangerously close to violating the privacy obligations imposed on us by law. For example, the Wiretap Act (also known as Title I of the Electronic Communications Privacy Act (ECPA) or Title III of the Omnibus Crime Control and Safe Streets Act of 1968) expressly protects wire, oral, and electronic communications while in transit and establishes that service providers are permitted to intercept those communications only as a necessary incident to the rendition of service or to the protection of the rights or property of the provider. Similarly, except as authorized by ECPA, section 705 of the Communications Act of 1934 makes it a crime for any person "to intercept and divulge or publish the contents of wire and radio communications" – a provision not limited solely to common carriers.

The Practical Realities of Technological and Legislative Solutions

The interdependent, interconnected, and global nature of the Internet means that areas of vulnerability exist throughout the network, and therefore cannot be realistically addressed by any single stakeholder. Given the rapid and ever-changing nature of the robocall problem, it is highly unlikely that a technological “silver bullet” can be developed as a permanent solution. Much in the same way that remediation efforts in areas such as spam or cybersecurity must continually evolve, the same can be expected for robocalls.

Robocalls, like their brethren in the area of spam, phishing, and cybersecurity is a constantly evolving problem. USTelecom supports the development of possible technological solutions to the robocall problem by stakeholders throughout the Internet ecosystem, most of whom are not constrained by the significant legal limitations currently facing our members. But members of this Committee need to be aware that no single solution will permanently address the robocall problem. Today’s solution could very well turn into tomorrow’s Maginot Line, and could have unintended adverse consequences.

For example, solutions that rely extensively on blocking calls populated by a blacklist could very well result in the blocking of legitimate calls from callers whose own phone numbers have been illegally spoofed. Conversely, solutions implementing call blocking features based upon a whitelist could potentially block an important – albeit unexpected – message from a legitimate caller. Even more perversely, the availability of spoofing technology can easily fool consumers into taking calls they should avoid. For example, spoofing the number of the local municipal hospital could dupe a senior citizen into believing that a fraudulent effort to sell phony medical products is actually a legitimate call from a whitelisted number. Given the open nature of the broadband network, technological solutions can be – and often are – superseded by technological countermeasures.

The same increasingly appears to be the case for legislative and regulatory solutions, which regrettably do not seem capable of keeping pace with the evil genius of scammers who continually invent new ways of evading discovery and capture, much less prosecution and punishment. As noted earlier, we have been trying to legislate out of existence the problems of robocalling, spam, autodialing, and caller-ID spoofing for as long as two decades, but new technologies only seem to make the problems grow worse.

Addressing Robocalling Requires A Multi-Pronged Approach

This is not to say that carriers are passive observers to the robocall problem. USTelecom's member companies work on multiple fronts in order to monitor, mitigate, and respond to mass-calling events. For example, many USTelecom member companies maintain network operations centers (NOCs), which include 24-hour security desks that monitor network traffic, respond to consumer complaints, conduct traffic data forensics, and initiate mass calling investigations.

In addition, carriers are providing – and will continue to develop – various services consumers can use to help mitigate the robocall problem. These services include basic caller-ID functionality, as well as conditional call-forwarding and anonymous call-blocking. Because the offerings and capabilities of companies are different, consumers are always encouraged to contact their respective service provider in order to identify available resources.

Network operators also work within the framework of various standards setting groups, the best example of which is the Alliance for Telecommunications Industry Solutions (ATIS). ATIS is a standards organization that develops technical and operational standards for the communications industry, including standards related to the handling of mass-calling events. In addition, several

USTelecom member companies are members of the Communications Fraud Control Association (CFCA). CFCA's membership consists of approximately 200 different carriers, private network owners, end users, law enforcement officers, and others from around the world. Through these public-private partnerships, industry stakeholders work together to identify best practices and solutions to a broad range of telecommunications-related issues, including robocalls.

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

Finally, the competition between our companies and other communications platforms for consumer and enterprise business provides incentives for all communications providers to innovate and to develop new and more effective solutions to challenges such as robocalling. This competition requires us to offer consumers the best possible experience subject to what the law allows us to do, including taking action to mitigate robocalling. If we do not offer effective solutions, consumers will simply migrate to alternate technologies that offer better ones.

In closing, let me again thank the Committee for holding this timely hearing. We share both the consumer's and Committee's frustration with the issue, and we look forward to our continued work together in a manner that provides flexibility in addressing this constantly evolving challenge.