Prepared Statement to the U.S House of Representatives

Energy and Commerce Committee

Communications and Technology Subcommittee

Modernizing the Telephone Consumer Protection Act (TCPA)

By

Richard Shockey

Shockey Consulting LLC

September 22, 2016

Chairman Walden, Ranking Member Eshoo and members of the Committee, thank you for the opportunity to speak with you today. My name is Richard Shockey and I am a telecommunications engineer by profession and the principal of Shockey Consulting LLC, a firm specializing in communications technologies, especially those involving the voice networks. In addition, I am Chairman of the Board of the SIP Forum. SIP, or the Session Initiation Protocol[1], is the fundamental Internet technology which all modern voice networks in the United States are designed around. Disclaimer: I am only speaking for myself here and my views may or may not be the same as those member companies of the SIP Forum.

We are all aware of the plague of Robocalls and Caller-ID spoofing. The two problems are linked. Many of us in the engineering community have been actively looking at this problem for many years now. Although there is no "Silver Bullet" here, better engineering can help and, in my humble opinion, there is engineering consensus on a path forward.

The "spoofing" problem, in which callers alter the calling party number information transmitted with their calls, is a key challenge for two reasons. First, any blocking or filtering tool that identifies unwanted calls based on the calling party number can be bypassed by bad actors who can simply spoof numbers not on the blacklist. This means that any particular blacklist-based blocking or filtering tool can be defeated by robocallers. And the more widely deployed a particular blacklist becomes, the greater the incentive robocallers have to find ways to bypass it. Unfortunately, some of the recipients of the robocalls with spoofed legitimate numbers will report the legitimate number as associated with the robocall. The innocent customer to whom the number is assigned can find himself or herself on a blacklist and, thus, subject to having his/her calls blocked. We have seen this problem in e-mail SPAM remediation

[1] https://www.ietf.org/rfc/rfc3261.txt

where a user's domain is blacklisted and the domain owner has no way of finding out who put them on a blacklist and, worse, no information on how they can get off a blacklist. I have personally dealt with that problem in the past.

Part of the overall solution involves applying modern Public Key Infrastructure (PKI) to cryptographically "sign" every signaling message for calls and, ultimately, text messages in the United States in a process we define as Call Validation. Some of these concepts have come out of the Internet Engineering Task Force (IETF), and its STIR working group, and the SIP Forum/ATIS Joint Task Force on Network to Network Interfaces.[2]

Second, we envision service providers could develop and eventually leverage modern data analytics technology and algorithms to attempt to determine if a call is a robocall or if it has been spoofed. This is the same class of data technology that the financial service industry uses to detect credit card fraud among others applications. On the basis of this data, we also envision that we could signal the consumer's telephone, or "user agent" as we call it, to display the results of this Call Validation Technology and empower the consumer to act accordingly.

We also want to offer businesses and individuals the option to enhance the identification information contained in the call presentation (what you see when you are asked to answer a call). We believe there is enormous value in having a trusted, validated identification accompany a call or message. This is especially important for both National Security, as well as Emergency Preparedness (NS–EP) applications.

This Committee is also aware that the robocall problem has an international dimension. Many of us in the engineering community believe that these Call Validation solutions may be adopted by other National Regulatory Authorities in a coordinated effort to combat the problem.

[2] http://www.prweb.com/releases/2014/SIPForum_NNI-TF/prweb12315811.htm

We know that much of the malicious traffic is coming from outside our borders and I believe these techniques can, and indeed must, be applied to international call/messaging gateways as well.

For those consumers that do not have modern mobile smartphones or internet protocol (IP) based desktop phones or have access to modern SIP networks, what do we do? I am trying to speak to the problem of, "What about Grandma?", "What about Aunt Phoebe?". This is a more complicated problem.

I believe Call Validation technology has positive benefits for our Law Enforcement Agencies that need effective "Track and Trace" mechanisms in the call signaling to track down the bad guys and shut them down.

I wish to emphasize that none of these technical solutions would inhibit a consumers ligitmitate desire to enable privacy options in call display (Anonymous) that are currently in place.

The Robocall Strike Force called by Federal Communication Commission Chairman Wheeler and Randall Stephenson, the Chairman of AT&T, is working on this engineering solution. Both Chairman Wheeler and Mr. Stephenson should be congratulated for this initiative, as well as all the companies that have agreed to participate. It is an extraordinary group of dedicated professionals. I am not a member of that Strike Force, but I am intimately aware of the technical inputs that the Strike Force is considering. Long ago the engineering community realized that part of the problem was that our voice communications system was a hybrid of classic Time Division Multiplexing/Signaling System 7, which is an ancient, decaying 30- to 40-year-old technology, and modern SIP technologies. This mix has contributed to weaknesses in the core voice network itself that have, in part, exacerbated the robocall spoofing problem.

Although there is no “Silver Bullet” here, better engineering can help. Implementing those solutions will require leadership from service providers, their suppliers, Congress and the Federal Communications Commission.

I understand the natural frustration that members of this Committee have with why these solutions have taken so long. It is complicated stuff. We have had to develop technologies that can be applied in the network while, at the same time, insuring the Security, Reliability, Integrity and Interoperability of the existing system. Though this is not exactly changing the tires of an airplane at 30,000 feet, there are elements that are similar. In addition, the telephone network is undergoing a “Technology Transition” from classic TDM/SS7 to SIP based networks that has been the subject of ongoing discussions at the Federal Communications Commission and here in Congress. I wish to emphasize that that Technology Transition needs to move forward with “all deliberate speed”, since many of the solutions the engineering community proposes cannot be fully applied to legacy networks.

This Committee is specifically looking at revising the Telephone Consumer Protection act (TCPA) to reflect modern realities, but the TCPA itself is not the only piece of legislation that is in desperate need of revision. The Truth in Caller-ID Act also needs to be revised. Robocalls are being facilitated because the call identification cannot be trusted. You cannot fix one problem without attacking the other. I am pleased to see H.R 2566 and H.R 2669 put forward. This is a fine start. In particular, H.R 2566 has proposed to require intermediate telephone call transit providers register with the FCC. I am deeply concerned that efforts to block robocalls do not complicate the ongoing problems of Rural Call Completion that this Committee is also concerned about.

The most important thing I can suggest to the Committee is that it express its intent to the FCC and our Law Enforcement Agencies with absolute clarity. The Commission should be authorized to investigate the feasibility of enabling new databases such as "Do Not Originate" and further rules that create indicators in the National Numbering Databases on when a number has been disconnected and when it could be available for reissuance. I would also like to see the FCC take further action on a proposal on what is often referred to as National Number Portability or the ability to take a telephone number and essentially keep it for life within the United States. 12 % of the US population moves every year and often have to disconnect a number when they move. [3] This would dramatically cut down on the volume of numbers being pulled out of service and subject to reassignment.

This is just another one of the issues in the voice network Technology Transition that are interrelated and interconnected.

I also note that the FCC made several recommendations in 2011, including regulating 3rd party spoofing services. I would suggest that Congress consider revisiting some of those recommendations as well.[4]

The engineering community is capable of giving the industry and our regulators the tools they need to combat this problem, but this Committee needs to make sure that they can use these tools under appropriate "Safe Harbor" provisions. We need to protect those industries that alert consumers with various messages that affect our financial security and personal health. Legislation needs to give protection to those businesses that act "In Good Faith" to contact their

[3] http://www.census.gov/newsroom/press-releases/2015/cb15-tps99.html

[4] https://apps.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.pdf

customer without the endless threat of nuisance suits or endless regulatory burdens that require more and more lawyers to create ever more complicated exemptions.

I am pleased to answer any and all questions and assist this Committee now and in the future.