Statement to the U.S House of Representatives

House Committee on Homeland Security

Cybersecurity, Infrastructure Protection and Innovation Subcommittee

Progress in combating Robocalls and Caller ID spoofing

By

Richard Shockey

Shockey Consulting LLC

April 2, 2019

Members of the subcommittee, 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 Northern Virginia 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.

I'm also a member of the Federal Communications Commission North American Numbering Council (NANC), which is the formal FCC Technical Advisory Committee on telephone numbering, and I have previously served on the FCC's Communications Security Reliability and Interoperability Council (CSRIC).

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. It is very appropriate for this subcommittee to look into these questions. Robocalls and Caller-ID spoofing are clearly forms of cybersecurity attack against the critical communications infrastructure of the United States.

Many of us in the engineering community have been actively looking at this problem for many years now. Although there is no "Silver Bullet", better engineering and technology is helping and, in my humble opinion, there is consensus on a path forward.

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

There is considerable good news here. Part of the overall solution involves applying modern Public Key Infrastructure (PKI) to cryptographically "sign" every signaling message for voice calls and, ultimately, SMS text messages in the United States in a process known as Call Authentication / Call Validation. We refer to this as the STIR/SHAKEN Framework.

These concepts have come out of the and the SIP Forum/Alliance for Telecommunications Industry Solutions [ATIS] Joint Task Force on Network to Network Interfaces and Internet Engineering Task Force (IETF), and its STIR working group.

STIR/SHAKEN has received the formal endorsement of the Federal Communications Commission under Chairman Pai's leadership. It has also been mandated for deployment by the Canadian Radio-Television and Telecommunications Commission, the telecom regulator of Canada.

ATT, Verizon, Comcast and T-Mobile have all made public statements over the last 60 days that they are in the process of STIR/SHAKEN deployment. Many other carriers have made formal declarations of support for the technology and have made written commitments to the FCC to deploy this year, if possible.

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. US Telecom, the trade association of the incumbent carriers has been leading its own task force in this area.

Concurrent with the STIR/SHAKEN initiatives, the voice engineering community has received wonderful support from the Federal Trade Commission and the Department of Homeland Security, which have supported these efforts through DHS Science and Technology Directorate by funding advanced research and development in this area. In addition DHS Cybersecurity and Infrastructure Security Agency (CISA) and its Emergency Communications Division have been instrumental in developing with the SIP Forum/ATIS Task Force Priority Resource Header protocols support to the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service for support to National Security/Emergency Preparedness users.

This funding is vital and needs to continue.

We still have many unanswered issues. In particular, how the STIR/SHAKEN data is passed to enterprises, public safety and critical infrastructure industries. In addition, we are continuing to debate what information should be passed to consumers and enterprises and in what form. We call this concept "Rich Call Data."

Though there is progress, I can't emphasize enough that there is no "Silver Bullet" here. It has been a multifaceted problem that will require multifaceted solutions for many years to come.

The bad guys have proven they are clever and relentless.

Vigilance, ladies and gentlemen, Eternal Vigilance.

There is other good news. There are two bills here in Congress that are addressing various robocall Caller ID Spoofing issues. In the Senate, Senator John Thune (R-ND) (Senate Whip) and Senator Ed Markey (D-MA) have a bill that is going into markup in the Senate Commerce Committee tomorrow, April 3rd.

Here in the House, the current Chair of the House Commerce Committee, Frank Pallone (D-NJ), has introduced a bill as well. Both measures increase fines for robocalls, extends the statute of limitations for prosecutions and gives the FCC clear and unambiguous Authority to Act to Mandate Call Authentication Call Validation technologies for every carrier. I believe further legislative and/or regulatory actions may be needed to protect STIR/SHAKEN data and other Call Validation signaling from malicious deletion or alteration in transit.

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

****