

Shockey Consulting

Richard Shockey
2427 Silver Fox Lane
Reston, Virginia 20191
Phone: +1 703 593 2683
E-Mail: richard@shockey.us
rshockey101
LinkedIn/Facebook/Skype
www.shockey.us

▶ VIA ECFS

February 24, 2015

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th St SW
Washington DC 20554

»

RE:

CG Docket No. 02-278 Rules and Regulations implementing the Telephone
Consumer Protection Act of 1991

WC Docket No. 07-135 Establishing Just and Reasonable Rates for Local
Exchange Carriers

Dear Ms. Dortch:

On Thursday February 19 2015, I participated on a panel on Voice and Telephony Abuse at the MAAWG Conference in San Francisco.¹ During the panel discussion I discussed my views on the issue of User Directed vs Carrier Directed Call blocking that was the subject of the recent US Attorney Generals petition.

On that panel were Patricia Huse of the Federal Trade Commission and Parul Desai of the Consumer & Government Affairs Bureau, Federal Communications Commission. Since this matter is still an open Docket at the FCC I'm submitting my presentation and additional reply comments per the Commissions rules.

I am the principal of Shockey Consulting LLC, a private firm in Northern Virginia advising telecommunications companies, technology suppliers, the investment community and national

regulatory agencies on any number of issues related to Voice over IP, PSTN Transition, Network Design and Architecture, Peering, Numbering and Signaling.

I am also Chairman of the Board of Directors of the SIP Forum an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology [IETF RFC 3261]. SIP is the principal technical protocol for Real Time Communications over residential, mobile, enterprise and carrier networks. The SIP Forum is also working closely with the Alliance for Telecommunications Industry Solutions [ATIS] on an industry wide Network to Network technical interfaces to facilitate the PSTN Transition. www.sipforum.org. For many years I was the co-chair of the IETF ENUM working group [IETF RFC 6116].

From 2011 to 2013 I was a member of the FCC Communications Security Reliability and Interoperability Council (CSRIC III) and have testified and filed before the FCC, the Canadian Radio-television and Telecommunications Commission (CRTC) and OFCOM in the United Kingdom on various technical matters.

My views in this letter and the attached presentation are solely my own and to not represent any view of the companies or participants of the SIP Forum.

The letter from the National Association of Attorney Generals [NAAG] raises important questions. I have reviewed most of the comments from various industry participants. The comments were universally thoughtful, technically accurate and represent a deep concern for what is an increasing menace to public safety.

I particular I want endorse the comments of US Telecom in this proceeding and re emphasize several of the excellent points made.

First: The problem has arisen due the very nature of the new modern competitive landscape for Real-Time Communications made possible by the enactment of the 1996 Communication Act. As new competitors entered the market, technology evolved and the cost of making a phone call dropped by orders of magnitude benefitting consumers and enterprises alike. The direct consequence of this is the Caller ID spoofing problem or in other words “No good deed goes unpunished”.

Second: The Commission needs to carefully note the difference between User Directed Call Blocking vs Network Directed Call Blocking. The PSTN already has User Directed Selective Call Acceptance (SCA- the white list) and its twin Selective Call Rejection (SCR – black list). Network Directed Call Blocking is sometimes referred to as “Do Not Originate” or “Super Do Not Call”. In particular the Do Not Originate would potentially allow the carrier to block any call that is using a non-allocated North American Numbering Plan NPA-NXX number.

The Industry is correct to point out that Network Directed Call Blocking has significant risks associated with it and may be illegal under the Commission’s current rules for “the call must go through”. Network directed blocking is not allowed even in cases of billing disputes. The industry is continuing to work thorough the contentious issue of Rural Call

Completion so complicating matters further without clear guidance or 'Safe Harbor' rules is ill advised. The potential for abuse of call blocking through black lists enormous.

Third: Internet engineers, such as myself, are looking at various technologies that could substantially suppress the problem of Caller ID Spoofing . We should all understand there is "No Silver Bullet" here. The IETF STIR initiative is one of those and industry, the FCC and the US Government need to support that effort with increased technical resources and public support. The STIR initiative, however will take time, and will eventually require substantial input from the Commission and US industry numbering committees.

I also support a national effort to provide consumers with more network centric validation and verbose identification to permit consumers and enterprises to answer a call with some level of confidence that the call is actually coming from a trusted source. I refer to this as CNAM Plus or Enhanced Calling Party Identification.

Fourth: Industry correctly reminds the Commission that we are undertaking a Transition of the PSTN to all IP technologies. It would be foolish in the extreme to ask the industry to deploy capital resources in a vain attempt to modify existing Class 5 Time Division Multiplexing [TDM] and Signaling System 7 [SS7] equipment that is already in some cases 30 years old and slated for decommissioning.

I would be happy to clarify any issues with staff if needed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Richard Shockey". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Richard Shockey
Principal
Shockey Consulting

CC: Parul Desai

Technical Options

MAAWG

Voice and Telephony Anti-Abuse SIG
San Francisco February 19-20 2015

Richard Shockey

Shockey Consulting

Chairman of the Board SIP Forum

[These opinions are my own not those of the SIP Forum or its members..usual disclaimers]

Reston, VA 20291

richard@shockey.us

Voice +1 703 593 2683

Skype/LinkedIn/Facebook – rshockey101

- The Spoofing problem needs to be understood in its larger context.
- The PSTN is undergoing a radical transition
 - With VoLTE IP based voice will be 75% of the market in 3 years.
- Existing PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL].
 - Your carrier goes to eBay for parts.
- Some of it is 30 years old. It cannot be modified.
- Competitive markets in part created the problem.
 - “No good deed goes unpunished”
- All IP Interconnection now a reality US CA EU
- SIP Forum and ATIS developing a Profile for all IP Interconnection.

2

How did we get here?

- There is no silver bullet to end Caller ID Spoofing.



3

But some Big Guns might help.

Regulatory – Technical - Legislative



- The inherent Circle of Trust among traditional carriers has been broken
- SIP signaling is ASCII text and as such is potentially subject to modification in transit by various network elements.
- As the Internet Architecture Board (IAB), noted,
 - “Without any form of cryptographic identity assertion, the ‘From’ header can be easily forged, and headers are often stripped or modified by intermediaries in transit.”
- Solution use Resource Public Key Infrastructure [RPKI] to SIGN SIP Signaling and create cryptographic keys for the entire North American Numbering Plan
- The IETF’s STIR Working Group is chartered to find solutions.
 - <http://datatracker.ietf.org/doc/draft-ietf-stir-problem-statement/>

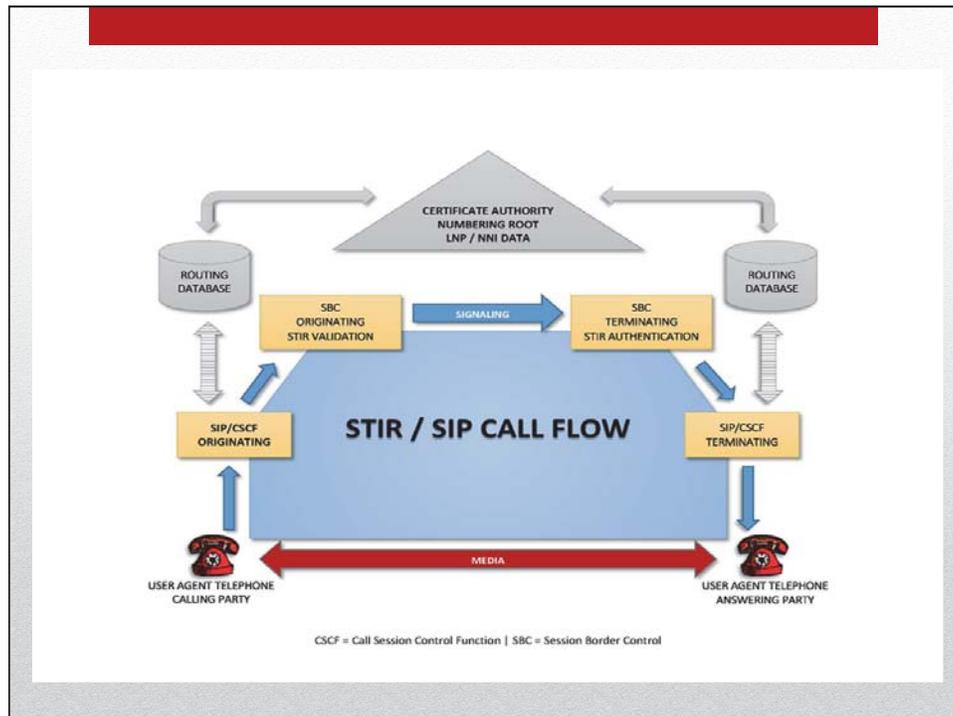
5

STIR

- The work profits from the fact that the assignment of phone numbers by national authorities is hierarchical, thus somewhat similar to assignment of IP addresses Autonomous System Numbers [AS] by RIRs ARIN RIPE APNIC etc.
- For the somewhat related problem of route hijacking, the implementation of Resource Public Key Infrastructure (RPKI) as the first phase of realization of Secure Inter-Domain Routing (SIDR) is widely viewed as the most promising technical means of mitigating the problem and securing the Border Gateway Protocol.
 - <http://datatracker.ietf.org/wg/sidr/charter/>

6

STIR

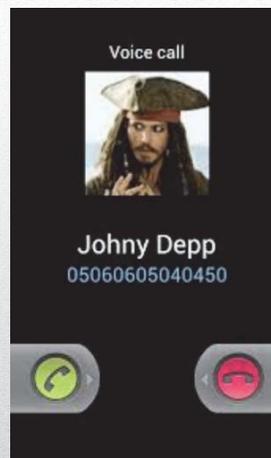


- Steps and likely time frames include:
 - SIP protocol enhancements.
 - X.509 certificate profile
 - Certificate Revocation List (CRL).
 - Selection of Cryptographic Material
- **Policy Question: When to begin regulatory consultations on Certificate Repositories. Who issues private keys? Where are the public keys stored? In the numbering databases? LERG NPAC?**
 - We do not want to see a repeat of Web SSL cert invalidation.
 - Actual implementation. The Session Border Controller (SBC) is the key to carrier implementation. At the conclusion of Standards development vendors would probably need 12 to 18 months to get something into a General Availability release, followed by at least a year of network operators testing.
- The entire process could take at least five years.
- IMHO STIR is both essential and inevitable.

8

How long will it take to implement STIR ?

- The issue is the Consumer has little or no information to on how to validate with confidence that the call is coming from where it was originated.
- In this day and age it seems silly that CNAM is still only 15 character ASCII.
- Potentially CNAM + . This could allow for a picture or logo of a bank to be displayed in the User Agent perhaps with network validated reputation data etc.
- Very serious discussion in the IETF, ATIS and 3GPP about this. Possible IETF WG formed soon.
- Integration with STIR



9

Enhanced CNAM

- The UK NICC Technical advisory is proposing a new technical requirement for operators. To be published very shortly.
 - <http://www.niccstandards.org.uk/>
- We know a lot of the malicious traffic is coming in from international call gateways.
- The Pseudo ANI/CLI idea now being floated to OFCOM would use a specific UK Number Plan range to identify “untrusted” or “unreliable” calls classified by the carrier coming in to the PSTN though a gateway.
- The Regulator or Numbering Administrator would maintain a WHOIS database of the numbers and what carriers use them.

10

Pseudo-ANI/CLI for International Gateways

- The proposed rules NICC/OFCOM may consider look like this.

Rule CLI NC 1

- a. On calls received from networks not covered by this specification (eg. international calls) the CLI information shall be classified by the receiving network as follows:
- b. When the Network Number is considered reliable then it shall be forwarded together with any associated classification.
- c. When the Network Number is considered unreliable or is absent the Network Number shall be set to a number from the range allocated to the CP receiving the call and classified CLI Unavailable.
- d. Any number that has the role of a Presentation Number in the incoming signaling system may be forwarded as the Presentation Number, with the associated classification. In the absence of a Presentation Number and where deemed appropriate the interworking operator may send the received Network Number as the Presentation Number.

11

Pseudo-ANI for International Gateways

- The issue of User Directed Call Blocking vs Network Directed Call Blocking which is what 36 United States Attorney General's have asked the FCC about.
 - The PSTN already has User Directed Selective Call Acceptance (SCA- the white list) and its twin Selective Call Rejection (SCR – black list)
 - Network Directed is sometimes referred to as “Do Not Originate” or “Super Do Not Call” In particular the Do Not Originate would potentially allow the carrier to block any call that is using a non-allocated NANP NPA-NXX number.
- **Policy Question.** The carriers will want some ‘Safe Harbor’ here due to existing “the call must go through” regulations etc.
 - Call blocking has become a very big issue in the US with Rural Carriers and Least Cost Routing Engines.
- The potential for DoS abuse is huge. Call blocking ex spouse
Girlfriend. Boyfriend. Employer.



Whitelist Blacklist for phone numbers

- Who actually 'owns' the number? Who is really the carrier of record?
 - WHOIS for Phone Numbers?
 - Blocks of numbers are passing through multiple carriers.
- What is that number actually used for?
- Central to this idea is a long term redesign of the entire NANP numbering scheme and what new numbering databases should look like.

- The Future of Numbering. [FCC March 2014]
 - Kudos to Henning Schulzrinne
 - <http://www.cs.columbia.edu/~hqs/papers/2014/2014-NumbTest.pptx>
 - Are Phone Numbers Domain Names?

 - My comments to the FCC on Numbering [March 2013]
 - http://shockey.us/index.php/download_file/view/13/142/

13

Future of Numbering

- Carriers will not spend ANY money trying to modify existing Class 5 TDM/SS7 gear in the network.
- The PSTN Transition actually makes spoofing enforcement technically easier
- We have about 3 years to put a plan in place
- It may be time for a little "jawboning" to help the carriers free up technical resources.
 - Chairman Wheeler, Chairwoman Ramirez and Chairman Blais need to be a bit more public about all of this.



Other observations