

February 21, 2015

Via ECFS

Marlene Dortch, Secretary
Federal Communications Commission
445 12th Street NW
Washington, DC 20554

RE: Notice of Ex parte, Dockets WC 07-135 & CG 02-278

Dear Ms. Dortch,

David Frankel, CEO of ZipDX LLC met with the following individuals in the Consumer and Government Affairs Bureau on February 19, 2015: Kristi Lemoine & Kurt Schroeder.

The discussion focused on the attached materials.

Regards,

/s/
David Frankel
CEO, ZipDX LLC
Monte Sereno, California
1-800-372-6535 / dfrankel@zipdx.com

cc: Meeting Participants, via E-mail

The Challenge of Robocalls WC 07-135, CG 02-278

David Frankel (dfrankel@zipdx.com)

19-Feb 2015

Terrorists Seizing US PSTN

- Robocallers have invaded the United States Public Telephone Network
- They invade the solitude of virtually all Americans
- They perpetrate fraud and malfeasance on the unsuspecting
- Hundreds of millions of Do-Not-Call entries are ignored
- TSR & TCPA are violated
- Billions of calls are being placed
- Robocallers operate with impunity; evading authorities is trivial
- Citizens are being asked to take up arms (blocking solutions)
- We need to take back our network from the terrorists!

Robocallers Devalue & Destroy the PSTN

- Dinners are disrupted and sleeping babies are awoken
- Millions report that they don't answer the phone because they don't want to endure a robocaller
- Implementation of "CAPTCHA" and other screening techniques
 - Delivers a miserable experience to legitimate callers
 - Presents additional barriers for those with disabilities
 - Impedes delivery of urgent and wanted messages
- What was a tremendously valuable resource meeting safety, business and social needs is devolving to a second class domain despite its unique position in reach, reliability and end-user accessibility

Caller-ID Based Blocking Approaches Fail

- Caller-ID is readily spoofable, including undetectable randomization
- Blacklists and whitelists are fundamentally problematic
 - Invitation for false negative and false positive results
 - Administratively impossible to maintain at scale
- IP-Based Authenticated ID is a noble long-term goal but it will NOT:
 - Even be selectively available for several years
 - Address the robocall problem until it reaches near-universal global adoption because robocallers will leverage any chink in the armor
- Near-term (next 2-10 years) robocall mitigation requires investment in other solutions

Robocalls Must Be Stopped @ The Source

- MILLIONS of calls can be initiated from a single call center / voice broadcaster / ACD in a few days or weeks
- Catching these at the receiving end is virtually impossible
 - There are hundreds of millions of endpoints of varying sophistication
 - Even at a cost of a few dollars (software) to tens of dollars (hardware) each, the aggregate cost would be BILLIONS of dollars and the timeframe extensive
 - Changes to receiving-end switches are also expensive and time-consuming
- There is no known way to reliably identify illegal or unwanted calls from signaling data
- Unlike with email SPAM, analyzing the media (voice path) is resource-intensive (so unscalable) and technically problematic

Complaint-Driven Traceback is Viable

- The FTC gets THOUSANDS of DNC / robocall complaints daily
 - Reports roll in promptly upon initiation of a new campaign
- If the report includes the approximate date & time and the called number:
 - We can use that info to go backwards through the networks to find the source
 - Individual carriers are already retaining (temporarily) the necessary data
 - We need “glue” applications that automate data retrieval and correlation
- Once the source (or at least ingress carrier) is identified, appropriate action can be taken to stop further calls
- This approach requires no end-point or switch changes and protects all end-users (even those that don't file complaints)
- Cost is relatively small (\$ millions) and fast for large impact
- There is precedent for government / industry cooperation like this

Discussion