Ex Parte Meeting Followup Filing

Regarding "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," FCC 16-39 (WC Docket No. 16-106)

Monday, June 13, 2016, 3PM Eastern

Attending:

Paul Vixie, CEO, Farsight Security, Inc.
Joe St Sauver, Scientist, Farsight Security, Inc.

Lisa Hone, Wireline Competition Bureau ("WCB"), FCC
Scott Jordan, Chief Technologist, FCC
Melissa Kirkel, WCB, Competition Policy Division ("CPD"), FCC
Sherwin Siy, WCB, CPD, FCC
David Brody, WCB, CPD, FCC
Alex Espinosa, WCB, CPD, FCC
Brian Hurley, WCB, CPD, FCC
Bakari Middleton, WCB, CPD, FCC
Gail Krutov, WCB, CPD, FCC
Brad Bourne, WCB, CPD, FCC
Andrew Field, WCB, Pricing Policy Division ("PPD"), FCC
Jeremy Greenberg, PPD, FCC

Preshared agenda for the call:

While Farsight filed 36 pages of comments about the NPRM, given the limited time available for today's call, Farsight wanted to focus on anonymized / aggregated data issues particularly relevant to Farsight. As such, Paul Vixie proposed the following agenda:

> [One definition: Properly aggregated/anonymized PI data ==> "P A/A PI D" ==> PAPID]
>
> 1. PAPID should generally be freely shareable
>
> 2. Close oversight by the FCC of PAPID is NOT needed
>
> 3. FCC should provide examples of satisfactory anonymization schemes
>
> 4. If those methods are used, FCC should provide safe harbor to data providers
>
> 5. We support the existing policy that permits:
>
> "telecommunications carriers to use, disclose, or permit access to aggregate customer information-collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed-without seeking customer approval."

Introductions were made.

FCC reminded Farsight that an Ex Parte filing would be required for the meeting. This was acknowledged.

The FCC noted as part of its opening remarks that some of the comments in Farsight's original filing, while on point from a practical point of view, are limited by statutory definitions (for example, enterprise networks are not in scope).

Farsight was then invited to begin their remarks.

-- Paul expressed appreciation for the opportunity to discuss Farsight's perspective. He noted that Farsight sent detailed comments, but given the limited time, wanted to focus on the matters particularly relevant to Farsight's business during the call, and that's around aggregated/anonymized data

-- There's always been a (perceived) tension between privacy and security

-- Paul recapped his anti spam background and experiences with MAPS, the Mail Abuse Prevention System

-- There's a need for security companies to look at metadata, but that needs to be done with due consideration of privacy concerns

-- Paul believes that Farsight has a system that collects as much as it can while not going over the line (this is a function of Farsight's architecture and the fact that it collects DNS cache miss traffic, above recursive resolvers)

-- Paul has worked extensively on DNS, and is of the opinion that DNS maps the Internet well, better, ultimately than BGP does. Farsight's focus is on what's happening, not the party making the DNS queries (that detail is obscured by the caching recursive resolver)

-- Other models for anonymization also can be noted. For example, Internet2, higher education's nationwide backbone, collects and shares network flow data, but anonymizes the low order 11 bits of IPv4 addresses and the low order 80 bits for IPv6 addresses.

-- The FCC asked if anonymization and aggregation is the same? FSI consensus was that while the two are complimentary, they are not synonymous. Paul noted that big data scientists possess an impressive ability to cross correlate multiple attributes associated with a single party's data to de-anonymize. Pooled data is far less problematic. (Difference between being able to see all the responses made by individual survey respondents vs. being able to see pooled responses for a set of respondents)

-- Discussion of DNS privacy -- are there examples where DNS may reveal PII? Because DNS is usable as a distributed database, some sites may choose to use it for distributed identity or license management. If when we notice this, we've filtered it from DNSDB and notified the party of the problem with that practice.

-- FCC asked about DPI, and whether that gives ISPs a unique (and hard to match) perspective. Farsight's perspective is that encryption is the answer: if you encrypt, DPI becomes moot. It was also noted that use of Tor, VPNs, or similar technologies has the ability to render customer traffic opaque to the ISP.

-- Paul also noted that the current focus on the BIAS may result in other parts of the Internet ecosystem filling in areas that may be forbidden to BIAS, but still permissible for other ecosystem segments.

-- Paul explained that Farsight's collection architecture (above the recursive resolver) means that we do not see "popularity" data for names. That is, once a name is resolved once and cached, all subsequent queries are resolved from the cached data until the DNS TTL "cooks down," at which point the next user's attempt to resolve that name will result in a new observable query to the authoritative name server.
result in a new DNS query.

-- Query from the FCC: has Farsight seen Peter Swire's paper on what ISP's know? [believed to be referring to this working paper: http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf]
Farsight: no we haven't, but we will review it.

-- Farsight explained that the concern is that ISPs, being risk adverse, may perceive restrictions that may not exist or be intended to apply, and may decline to share security-critical data as a result.

-- FCC wondered if there's really a cause for concern in the NPRM with respect to the data that Farsight is collecting given existing carve offs (such as the one mentioned in the proposed topics for the meeting). The issue may just be one of "translation" or "interpretation."

-- Question from the FCC around Farsight's comments around e-pending: Farsight is concerned with e-pending as a general privacy issue because it undercuts consumer control and allows a marketing company to accumulate a dossier about users even if just given scant starting points. It is also a practice that's explicitly rejected by legitimate email service provider norms, such as those from the Messaging, Malware and Mobile Anti-Abuse Working Group (m3aawg.org). [reference was to this document https://www.m3aawg.org/sites/default/files/document/MAAWG_Epending_Position_2011-09.pdf]

Meeting concluded at 3:50PM Eastern.