From: Alan Greenberg
Date: Friday, April 20, 2018 at 16:59
To: "gdpr@icann.org"
Subject: [Ext] Comment from Alan Greenberg on the Article 29 Letter

This is being submitted on my own behalf.

The letter shows an astonishing lack of understanding of ICANN's mission.

The Article 29 letter says *"Finally, ICANN should take care in defining purposes in a manner which corresponds to its own organisational mission and mandate, which is to coordinate the stable operation of the Internet's unique identifier systems. Purposes pursued by other interested third parties should not determine the purposes pursued by ICANN. The WP29 cautions ICANN not to conflate its own purposes with the interests of third parties, nor with the lawful grounds of processing which may be applicable in a particular case."*

From ICANN's Bylaws: The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems…

Implicit in this is to ensure that the DNS is trusted. Without trust, it is meaningless. Why would you ask the DNS to translate a domain name into and IP Address if you did not fully trust it?

Our mission is not just a mechanical collection of data about Domain Names. Ensuring trust in the DNS *IS* our mission.

If we ignore the uses that law enforcement, cyber abuse fighters, etc. make of WHOIS, we cannot COLLECT the data they need. If it isn't collected, it cannot be used, no matter who later justifies the need!

If ICANN, the only body that can set the rules for what is collected, cannot do so, the parties who COULD justify the use of that data have nowhere to make their case.

There is no doubt that we need to beef up the rationales for collecting data, but it is a useless exercise if we cannot ensure that the DNS can be properly policed and protected.

On one other issue, the Article 29 letter applauds anonymized e-mail addresses. Although there are some issues relating to whether anonymized addresses are reliable (if an address fails, you get no feed-back as to why), there is a more critical issue. E-mail addresses are used to recognize patterns in DNS abuse (and in IP violations with the UDRP and URS). Anonymized addresses can be used, but ONLY if the same e-mail address always translates to the same anonymized address (specifically across multiple registrations and multiple registrars).

Alan Greenberg