Dear all,

I will not be able to join the call tomorrow so I thought that I should email the list to explain why I voted against the proposed possible WG Agreement according to which "*Criminal Activity/DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but maybe a legitimate purpose of using some data collected for other purposes*."

I think that there are a number of rationales/grounds - including ICANN's Bylaws - to argue that in fact, investigating criminal activity and DNS Abuse **IS** a legitimate purpose for requiring the collection of registration data.

Some of these rationales have been mentioned during the discussion on the mailing list and during the call on 9th January. Unfortunately, I think that the proposed possible WG agreement does not take into consideration these rationales. I specifically disagree with the assumption that we should make a distinction between 1) the purpose of collecting the data and 2) the purpose for using the data collected for other purposes (manage domain registrations).

The reason why I disagree with making this distinction is that it leads to artificially reduce the importance of a valid and legitimate purpose of the WHOIS system, acknowledged by ICANN Bylaws: addressing malicious abuse of the DNS and providing a framework to address appropriate law enforcement needs. (ICANN's mandate is to "ensure the stable and secure operation of the internet's unique identifier systems" 1 + WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."2). In its document on the three compliance models issued last Friday3, ICANN has explicitly included: addressing the needs of law enforcement, investigation of cybercrime and DNS abuse as legitimate purposes of the WHOIS system.

If one of the purpose of the WHOIS system is to support a framework to address issues involving domain name registrations, including investigation of cybercrime and DNS abuse, it can be argued that investigating criminal activity and DNS Abuse IS a legitimate purpose for requiring the collection of registration data. Likewise, I think that requiring collection of data to prevent crime is NOT beyond ICANN's mandate.

Best

Greg

Here is a list of relevant references supporting this point of view taken from ICANN's Bylaws and the GDPR:

1) ICANN's Bylaws support the conclusion that WHOIS services should serve the legitimate needs of law enforcement and promote consumer trust and as noted in Hamilton memo #3: "it would be incorrect to state that the only purpose of the Whois services is to manage domain name registrations."[4] .

[1] ICANN Bylaws Article One, Section 1.1, Mission.
[2] ICANN Bylaws, Registration Directory Services Review, §4.6(e).
[3] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[4] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en

2) ICANN's Bylaws, revised in 2016, make clear that ICANN's mandate is to "ensure the stable and secure operation of the internet's unique identifier systems."[5]

3) Further, ICANN's Bylaws include a commitment to preserve and enhance "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[6]

4) Finally, ICANN's commitments and required reviews emphasize that it must "adequately address" issues related to "consumer protection, security, stability, resiliency [and] malicious abuse."[7]

5) Regarding registration data specifically, ICANN's Bylaws recognize that WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."[8]

6) The GAC has also recognized these important purposes in its recent advice reflected in the Abu Dhabi Communiqué, noting that WHOIS data is used for a number of legitimate activities including: assisting law enforcement authorities in investigations; assisting businesses in combatting fraud and safeguarding the interests of the public; and contributing to user confidence in the Internet as a reliable means of information and communication.[9]

7) In addition, ICANN Bylaws require it to use commercially reasonable efforts to enforce its policies relating to the Registration Directory Service, while exploring structural changes to improve accuracy and access to generic top-level domain registration data, as well as considering safeguards for protecting such data. In fact, to the extent law enforcement and cyber security professionals use publicly available WHOIS data to detect and combat threats to the infrastructure of the DNS, the collection and disclosure of this data to these groups is essential to ICANN's core mandate: the security of the DNS and the Internet.

8) These public and legitimate interests are consistent with the GDPR, which permits processing (including collection) of data where necessary for the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by the controller or by a third party, subject to conditions, Art. 6(1)(e) and (f).[10] The third Hamilton memo also supports this conclusion: "Processing of Whois data by law enforcement agencies for such law enforcement purposes should

---

[5] ICANN Bylaws Article One, Section 1.1, Mission.

[6] ICANN Bylaws Section 1.2 (a) Commitments and Core Values.

[7] *See* ICANN Bylaws Section 4.6 (d), Specific Reviews, Competition, Consumer Trust, and Consumer Choice Review.

[8] ICANN Bylaws, Registration Directory Services Review, §4.6(e).

[9] ICANN60 GAC Communiqué, available at https://gac.icann.org/contentMigrated/icann60-gac-communique. P.11

[10] Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119/1, available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

constitute a legitimate interest that motivates processing of personal data in accordance with Article 6.1(f) GDPR.[11]

9) I include below for your reference the corresponding recitals explicitly mention in the GDPR:

   - "preventing fraud";
   - "ensuring network and information security," including the ability of a network or information system to resist "unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services," and
   - reporting possible "criminal acts or threats to public security" to authorities.[12]

[11] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en
[12] *See GDPR* Recitals 47, 49 and 50.