BC Comment on the Hamilton Memo regarding GDPR, as of 15-Jan-2018

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:

The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

BC Comment on the Hamilton Legal Analyses

The BC thanks ICANN and the Hamilton law firm for its time, effort, and legal analyses regarding compliance with the European Union's (EU) General Data Protection Regulation (GDPR).

However, as detailed below, further analysis is necessary *before* Hamilton analyzes proposed models for compliance with the GDPR as well as ICANN contracts, and *before* ICANN or members of the community can rely on these analyses to a model for GDPR compliance.

The BC makes a number of observations related to Hamilton's analyses, as follow:

Territorial Scope

Hamilton's analyses is missing key language -- the GDPR applies not to any processing that is done by a company that happens to have an establishment in the EU, but to processing done "in the context of" such an establishment.

Thus, this sentence from Section 2.1.1 of Hamilton's 15 December 2017 memo (Memo #2) is incorrect:

> *Therefore, all processing of personal data is, no matter where it is carried out, within the territorial scope of the GDPR as long as the controller or processor is considered established within the EU; the nationality, citizenship or location of the data subject is irrelevant.*

The correct statement would be this:

> *Therefore, all processing of personal data is, no matter where it is carried out, within the territorial scope of the GDPR as long as **it is done within the context of** a controller or processor's establishment in the EU; the nationality, citizenship or location of the data subject is irrelevant.*

Similarly, it is not, as Hamilton concludes that it is, "the establishment or business actions of the controller or the processor that determines whether or not the processing falls under the territorial

scope of the GDPR."[1] Rather, it is whether the data processing activities fall within the context of such establishment.

This is important because it defines the scope of applicability for the GDPR and dictates whether or not the GDPR applies in the first instance -- casting a wider net than legally necessary is unadvisable.

Consent

Hamilton concludes that consent is not a practically viable legal ground for processing personal data in an efficient way. This, however, is a qualified statement that shouldn't be taken to mean consent is not a legal ground for processing personal data, particularly as it relates to the publication of data through a data subject's unambiguous consent. The BC believes this is an important point that should not be overlooked. We recognize that there are instances whereby businesses and individuals will seek to have personally identifying information data made publicly accessible (e.g., to facilitate contact, or to accommodate sales or transaction inquiries) and Hamilton should provide additional guidance regarding how consent can be preserved within a model selected to stay GDPR compliant under such instances.

Public Availability of Email Addresses

The BC disagrees with Hamilton's conclusion that e-mail addresses should not be included in public Whois and that it would be "sufficient" to rely on a registrant's name and address for contact. This is inconsistent with and ignores the operational realities of the DNS, including the transfer processes, that enable competition among registrars, and the UDRP. Moreover, Memo #3 acknowledges Case C-398/15 (Manni) and, like the company registry at issue in the Manni decision, publicly available WHOIS data is essential to the proper functioning of the online marketplace -- being consulted by individuals and companies daily for various business and transactional purposes. Manni would seem to say that the publication of e-mail addresses under these circumstances would also be justified.

Law Enforcement Agency (LEA) Access

The BC finds Hamilton's analyses of LEA access (Memo #3 Section 2.6.4) overly restrictive and unsupported by laws that apply to ccTLD registries. Such over-restriction would unnecessarily curtail procedures that are universally accepted by the domain name community and are employed and relied upon by LEAs (and affirmed as necessary by the European Council's 7 November 2017 conclusion)[2] to address harms that jeopardize the security and stability of the domain name system. In addition, because the timeliness of data access is often critically important to law enforcement and network security response, any solution that contemplates the opinions and decisions of the Courts as part of a workflow is likely untenable. Moreover, it is concerning that Hamilton came to its conclusions based on cases it acknowledges "concerned different kinds of data for different purposes than what is the case in relation to the Whois services"[3] -- seemingly making the cases inapplicable to the analyses. Separately, the BC would like to note that law enforcement community often uses historical Whois data in its investigation and enforcement activities and this serves as justification for data retention as noted in Section 2.35.2 of memo #2.

---

[1] Id. Section 2.1.4

[2] 44. STRESSES the importance of ensuring a coordinated EU position to efficiently shape the European and global internet governance decisions within the multi-stakeholder community, such as ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded

[3] Hamilton Memo #3 Section 2.6.4

Whois Data Accuracy under GDPR

Hamilton's memo omits discussion of the requirement for data accuracy correction, and rectification under GDPR. Any model selected by ICANN must contemplate how to include a process that promotes accuracy and ensures that WHOIS data is verified and validated upon intake and thereafter -- whether published publicly or not. Moreover, Article 16 of the GDPR provides the right to rectification of inaccurate personal data. We offer that publicly accessible WHOIS furthers these requirements by allowing data subjects to easily confirm what data is held about them and where their data is erroneously or fraudulently used without their consent.

DPIA Consultation

The BC finds intriguing Hamilton's suggestion that ICANN submit to a DPIA to assess the impact of its selected model. Were ICANN to do so, however, it's critical that the community be given the opportunity to first evaluate and comment on the materials proposed for submission to such an assessment.

Conclusion

Many important business operations depend upon public availability of WHOIS, such as the ability to obtain digital certificates, or the ability to protect against spam, fraud, and other types of online abuse. The public availability of WHOIS enables reputational analysis used by security companies, online platforms, browsers and other services that collectively protect the Internet and its users from malicious conduct.

ICANN is required, under its policies, to arrive at a solution that, to the greatest extent possible, preserves the ability of the registrar/registry to comply with its contractual WHOIS obligations.[4] In so doing, it must keep in mind "the anticipated impact on the operational stability, reliability, security, or global interoperability of the Internet's unique identifier systems."[5] Too restrictive a model will detract from this capability and may adversely impact the overall security and stability of the Internet. The BC therefore renews its request for additional analysis in light of these comments (and others that may be received by ICANN).

At the same time, the BC is encouraged by the diversity of approaches reflected in the models submitted on January 10th for consideration, and recommend that ICANN publish all of them for public comment and further analysis by Hamilton.

--

This comment was drafted by Margie Milam and Tim Chen.
It was approved in accord with the BC Charter.

[4] See Revised ICANN Procedure For Handling WHOIS Conflicts with Privacy Law Section 2.1

[5] Id. at 4.1