ICANN Business Constituency (BC) Questions for Hamilton's legal analysis of GDPR and Whois

14-Nov-2017

Regarding Section 3.2.1: The GDPR has extended territorial scope compared to the Data Protection Directive and Article 3 GDPR sets out that it, in addition to being applicable to controllers and processors established in the EU, will apply to controllers and processors not established in the EU when their data processing activities are related to "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union".

Question 1: Are companies that offer services only to organizations and not to individuals excepted from (a) above, since the service is not given to a 'data subject' who by definition of GDPR is a natural person?

Question 2: Is behavior online necessarily behavior in the EU? Example: If an individual in Germany changes the IP address of his/her domain name, and that IP address is not hosted in the EU, is that considered 'behavior that takes place in the EU"? Can this be clarified, please?

Regarding Section 3.8.4.3: Looking at the current Whois services, there are several uses that could qualify as legitimate interests. For instance, recital 47 GDPR specifically mentions processing necessary for preventing fraud as a legitimate interest. And the Article 29 Working Party indicated that the "combatting of file sharing" could constitute a legitimate interest. So it can be argued that the following purposes of processing could constitute legitimate interest under Article 6.1(f) GDPR:

> (i) The use of Whois data, for instance by registrars and network operators, for invoicing, support and other administration actions in relation to registered domain names.
>
> (ii) The use of Whois data to investigate criminal behavior which could include: child online exploitation; phishing scams that exploit individual users; other forms of online fraud, consumer deception, abuse of trademarks or other
> intellectual property violations, or other violations of law.
>
> (iii) The use of Whois data to verify the identity of a provider of goods or services on the internet, including for consumer protection purposes and to allow a consumer to validate the authenticity of the offering company.
>
> (iv) The use of Whois data to identify the owner of a domain for business purposes, for instance in relation to a purchase of the domain name or other transactions.

Question 3: Are the purposes above considered "legitimate interests" under Article 6.1(f) GDPR?

Question 4: Would item (ii) above apply only to matters that are a "violation of law"? That is, is it a legitimate use of Whois to prevent consumer deception with the understanding that not all consumer deception may have an applicable law against it?

In its Bylaws, ICANN acknowledges its commitment to "(i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and

openness of the DNS and the Internet". Whois is critical to enabling those who combat fraud and abuse of domain names.

Question 5: How can ICANN assure that essential access to Whois will enable the legitimate interests described above?

Question 6: Can a Code of Conduct be developed by ICANN to apply to WHOIS? Please describe the pros/cons of using a Code of Conduct approach? Are there any industries or companies contemplating a code of conduct approach or have taken steps to put together a Code of Conduct?

Question 7: How can ICANN seek a public interest exemption, and under what circumstances have such an exemption been recognized? Is there any guidance on what is meant by the "public interest"? How are real estate ownership records or corporate registration registers able to comply with GDPR? (See for example, the CJEU's 2017 decision in Manni, involving the corporate insolvency records posted in a publicly available Italian register).

Question 8: EU law requires public WHOIS for domain names (ccTLDs) – recognizing the public interest served by having this information publicly available. Is there any case law or opinion that would indicate that the rationale for these laws would not also be applicable to gTLDs? (See the Finnish Domain Name Act and European Commission regulations No. 733/2002 and No. 874/2004.

A public WHOIS database is necessary for the performance of a contract - it is a requirement placed by ICANN for the registration agreements between registrants and registrars, as well as under the RAA and the Registry Agreements. ICANN's bylaws mandate a periodic review of Registration Directory Service, to "assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data."

Question 9: Are there any cases where provisions of industry-wide agreements have been challenged for failing to comply with the EU privacy laws? Is there any guidance on how to interpret "necessary for the performance of a contract"?