Input to ICANN's Proposed Interim Model for GDPR Compliance

March 8, 2018

As a global, multi-faceted technology corporation, Microsoft naturally has a wide variety of interests in ensuring the continued availability of the existing WHOIS system: we are a registry operator in relation to our own Top-Level Domains, we are an accredited registrar, and we use WHOIS data to protect our company and our customers. As outlined in our input to ICANN's July 2017 consultation[1], we rely on WHOIS data to investigate digital crimes, to detect network security threats, to enforce against infringements of our intellectual property rights, and to validate domain ownership when managing requests for Secure Sockets Layer (SSL) certificates or when facilitating domain registration and management workflows for internal colleagues as well as third party customers.

These uses of WHOIS data were recognized by the European Commission[2], when it "underline[d] the importance of … public policy objectives" achieved via use of WHOIS by government and non-government actors, "e.g. through … help in countering intellectual property infringements, finding the source of cyber-attacks or assistance to law enforcement investigations".

At Microsoft, we believe privacy is a fundamental human right and that the EU's General Data Protection Regulation (GDPR) is a major step forward in enhancing and securing the privacy rights of individuals. We also believe in the vital importance of maintaining a stable and secure Internet, which is central to ICANN's purpose, and which would be undermined by a reduction in the quantity and accessibility of WHOIS data.

We therefore support ICANN's goal of "ensuring compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible". It is important to find solutions which do not undermine the ability of all - ICANN, registries and registrars, legitimate users of WHOIS data - to comply with the GDPR.

This is certainly achievable given that the GDPR allows for uses of data for the public interest and legitimate purposes, lawful bases upon which WHOIS data can continue to be made available. In several ways, however, we find ICANN's Proposed Interim Model[3] unnecessarily cautious, silent or restrictive. If not revised in the final model, this will gravely hamper Microsoft's ability to protect our customers, and more broadly to help protect the stability and security of the Internet.

We have outlined specific concerns and recommendations in the two sections below on data access and data collection and availability. We are of course willing to provide further information should that be helpful, and we will continue to closely follow the discussions in the coming weeks, hopeful that solutions can be found to avoid the potentially damaging consequences outlined below.

---

[1] https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-microsoft-24jul17-en.pdf
[2] Letter of 29 January, https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf
[3] https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf

Data Collection and Availability

We welcome several significant aspects of the Proposed Interim Model, in particular that:

- there would be no change to the amount and nature of data elements that registrars would be required to collect and pass on to registries and data escrow providers;
- there would be no change to the length of time registrars must retain the registration data under the 2013 Registrar Accreditation Agreement (RAA) (for two years beyond the life of the domain name registration);
- there would be no change to the data accuracy (verification and validation) requirements that registrars currently need to comply with under the 2013 RAA in order to ensure that the WHOIS databases function properly.

However, we also have a number of substantial concerns about restrictions ICANN proposes to introduce in this model, in comparison to the current WHOIS system. Our most serious concerns relate to:

- the application of the model to all persons, without distinction between "natural persons" and "legal persons";
- access to the registrant's email address; and
- the importance of providing for the continued ability to access historical data and to access data on a searchable and aggregated (bulk) basis.

The Proposed Interim Model should only apply to data of "natural persons". In fact, data of "legal persons," to the extent such data does not reflect "personal data," is not within the scope of the GDPR. Accordingly, we disagree with ICANN's proposal not to require a distinction between data of natural versus legal persons. Instead, **the interim compliance model should require such a distinction between natural and legal persons**. To treat registrations of natural and legal persons the same would be overly broad, surpassing even the European Commission's own interpretation of the GDPR[4].

The registrant's email address is a critical data element for investigating cybercrimes and detecting nefarious behaviour in order to protect users and to secure networks, as well as in investigating infringements of intellectual property. For example, given that malicious entities rarely control only one domain name, the email address is a key means of correlating various domain names registered by a single registrant, known as "Reverse WHOIS"). It is also used to contact domain owners to inform them when their domains have been hijacked by others to carry out online attacks. Therefore, the **registrant's email address should be widely and quickly accessible**. Until there is an established accreditation program which provides quick and continuous access to public and private entities which have demonstrated legitimate purposes (as discussed in the following section), the importance of this data element means that ICANN should continue to require it to be made publicly available.

We are also very concerned that, under the Proposed Interim Model, contracted parties would not be required to provide searchable (Reverse WHOIS) or historical WHOIS data to any party, whether accredited or not, and would only be required to provided third-party bulk access to the (much more limited) public WHOIS data. While this is not a current requirement of the WHOIS system, the fact

[4] As noted on page 3 of the European Commission's technical input, https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf

that the data is currently made available in public WHOIS means that third parties are able to provide services which allow access to searchable and historical data.

Another important feature of the current WHOIS system is the ability to gain bulk / aggregated access to full WHOIS data. Malicious online activity often impacts large numbers of people almost simultaneously, so investigators must be able to rapidly analyze bulk and historical data to help identify key participants in the attack and map the infrastructure controlled by the responsible domain name registrant(s).

It is therefore critical that **any accreditation program requires WHOIS registries to provide for access to full WHOIS data on an aggregated, searchable and historical basis**.

Data Access

Microsoft accepts that compliance with GDPR will mean that some data will no longer be made publicly available. We therefore welcome the Proposed Interim Model's principle that accredited parties would have continued access to full WHOIS data, even if we believe the Model does not yet provide for all the data elements necessary for the various legitimate purposes described above.

However, there remain many elements of such an approach to be resolved before we can have confidence that this would enable us to continue to protect our customers and contribute to the security of the Internet. The accreditation approach will only work if a number of key factors are taken into account:

- It must be open not just to government authorities but also to a wide array of private bodies which serve various legitimate and important purposes.
- The program should provide a high standard of security, performance and reliability commensurate with the global scale of the Internet.
- The need for accreditation should not introduce delays to the process of accessing data given the critical time constraints of cybersecurity actions which rely on urgent action and real-time access to WHOIS data wherever possible. For example, real-time access to WHOIS data helps lower the success of domains created solely for criminal purposes, such as phishing, by surfacing anomalies in the WHOIS data elements to identify domains intended for abuse which can then be blocked at the email service layers.
- The accreditation program should therefore provide legitimate users with broad, persistent access to data for legitimate purposes, rather than having to be validated / authorized for every single WHOIS data request. This could be achieved by a centralized accreditation database, as ICANN suggests, although the system would need to ensure that, once accredited, an operator should not be burdened with further data access limitations.
- The time taken to design and implement an accreditation program should not lead to a period where the data cannot be accessed. If a program is not operational once the GDPR enters into force on 25 May 2018, a self-certification system should be put in place during the interim period so that the ability, for example, to protect Internet users and address security threats does not suddenly evaporate.
- The accreditation program should provide for an appeal process should a party's request for accreditation or for specific data be denied.