The ICANN GNSO "Business Constituency"

March 2021

Executive Summary

Access to domain name registration data – identifying information for the individual or organisation owning a website – is vitally important for public authorities and private organisations involved in law enforcement, consumer protection, cybersecurity and the protection of intellectual property. However, access to this data (also known as WHOIS data) is becoming more difficult, impeding critical investigations.

This is the subject of Article 23 of the draft Directive, which provides important clarifications on the critical value of WHOIS data, and when, how, and to what extent that data should be made available to third parties with a legitimate interest. These provisions are very welcome. However, a number of amendments are necessary to clarify and strengthen the text in order to achieve the Commission's important aims – improving further the resilience and incident response capacities of public and private entities in the field of cybersecurity and critical infrastructure protection.

Views of the ICANN Business Constituency on the NIS2 Directive

The ICANN Business Constituency (BC) writes to provide views on the European Commission's proposal for a revised Directive on Security of Network and Information Systems (NIS2 Directive), specifically in relation to domain name registration data (Article 23 and related definitions in Article 4).

The Internet Corporation for Assigned Names and Numbers (ICANN) manages the Internet's unique identifier systems, including the domain name system (DNS), with the goal of ensuring the stable and secure operation of the Internet. ICANN's multistakeholder policy development model for DNS management involves designated stakeholder groups. The BC is the voice of commercial Internet users within ICANN, representing the interests of small, medium, large and multinational enterprise users of the domain name system.

As such, we have specific interest in Article 23 of the draft NIS2 Directive on domain name registration data. Every year, millions of individuals, businesses, organisations and governments register domain names. Each must provide identifying and contact information which includes name, address, email, phone number, and administrative and technical contacts. This information, often referred to as "WHOIS data", is managed by entities known as "registrars" and "registries", described in Articles 4(14) and 4(15) respectively of the draft Directive.

The importance of access to WHOIS data

Cybercriminals rely on domains to launch coordinated and automated attacks on a global scale and to perpetrate a plethora of consumer fraud and scams. Accessing WHOIS data – the authoritative record of domain ownership – is the only viable means to obtain the information necessary to identify criminal actors, prevent harms and protect the online ecosystem. It is the only reliable accountability mechanism in an otherwise-anonymous internet.

As the European Commission noted in the July 2020 Communication on the EU Security Union Strategy, access to WHOIS data "is important for criminal investigations, cybersecurity and consumer protection", as demonstrated in the following examples:

- Cybersecurity professionals use WHOIS data to disrupt malicious attacks by identifying the email address registered to a malicious domain and then using "Reverse WHOIS" searches to identify all other domains linked to that email address, which might therefore also be used in the same or other attacks.
- Malicious online activity often impacts large numbers of people almost simultaneously, so investigators must be able to rapidly analyze massive amounts of current and historical WHOIS data to help identify key participants in the attack and map the Internet infrastructure that they control and deploy.
- Attackers often use domain names that are similar to major brand names. These domains are often used by hackers to communicate with malware installed on targeted computers, defrauding innocent consumers into trusting the names and links who then suffer phishing identity theft and other online scams. Accessing WHOIS data enables companies to bring action against domain owners for trademark infringement and reclaim offending domains. The companies are then able to observe and strategically disrupt hacking operations.
- Increasingly, criminals take control of legitimate servers or websites and leverage them for malicious purposes. Without ready access to detailed WHOIS information, cybersecurity professionals must treat all malicious domains as being owned by criminal actors, thus increasing the possibility of collateral damage from actions taken.

The need for legal clarity around the management of, and access to, WHOIS data

Over the past three years, following the entry into force of the General Data Protection Regulation (GDPR), a multistakeholder policy development process within ICANN has developed new policies on the publication of and access to WHOIS data. The BC and other ICANN constituencies, including the Governmental Advisory Committee (GAC) which represents national governments at ICANN, found the resulting policy recommendations to have failed the needs of cybersecurity, consumer protection, and law enforcement authorities as well as intellectual property rights holders due to misapplication of the important privacy protections created by GDPR.

The BC and other dissenting stakeholders expressed, and still maintain, strong support for privacy protections for personal data and are invested in the development of ICANN policies that balance the individual right to privacy with safeguards for law enforcement and other legitimate interests. But we agree with the GAC, which withheld support for certain new policy recommendations precisely because they "do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars and protecting the public from harms associated with bad actors seeking to exploit the domain name system."[1]

Benefits of the draft Directive and ways in which it can be clarified or strengthened

The provisions set out in Article 23 of the draft NIS2 Directive provide an important clarification on the critical value of WHOIS data, and when, how, to what extent that data should be made available to third parties with a

[1] See page 122 at https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtldregistration-data-2-31jul20-en.pdf. Note that this document also contains similar concerns from four other parts of the ICANN multistakeholder community - the At-Large Advisory Committee, the Security and Stability Advisory Committee, the Business Constituency and the Intellectual Property Constituency.

legitimate interest. It is supported by definitions in Article 4 and by recitals that explain the desired objectives of Article 23. In particular:

- The BC has frequently noted the difficulty of creating effective Internet Governance policies given a lack of explicit acknowledgement of the legitimate interest of third parties in requesting and further processing these domain name registration data records; Article 23(5) largely addresses this gap, although there is some ambiguity in the text that needs to be addressed.
- The requirements for accuracy in Article 23(3) and for prompt publication of non-personal data (including legal person contact data) in Article 23(4) are welcome, as they address a policy area that has proved extremely challenging for ICANN to resolve: the distinction between natural and legal persons when processing contact data.
- The obligations for processing and publication of WHOIS data by registries – as opposed to just registrars – rightfully recognises the critical part they can play in enabling access to WHOIS data. In the same spirit, the provision could be further clarified to include other entities providing services related to domain name registration, namely domain name resellers and privacy/proxy registration services. Also, in order to ensure a baseline for uniformity and consistency, it is important to add definitions in Article 4 to describe both DNS abuse and the elements that comprise "complete domain name registration data".

While these provisions are therefore very welcome, in order to prevent unintended consequences and ensure that the NIS2 Directive will enable timely access to accurate and complete WHOIS data for legitimate purposes, we offer specific suggestions and support to help strengthen the text in the following areas:

- Clarify the scope of DNS providers considered under Article 23;
- Allow for dedicated cloud service tenants as a place for collection and maintenance of domain name contact data;
- Address the use of privacy or proxy registration services to conceal the data of the person or organisation using the domain name;
- Ensure timely access to WHOIS data; and
- Recognise that legitimate access to domain name registration data serves the public interest.

This document was approved in accord with the Charter of the ICANN Business Constituency[2].

[2] https://www.bizconst.org/charter