ICANN | IPC

18 March 2021

Input on the Proposed Revised Directive on Security of Network and Information Systems (NIS2)

Introduction

The Intellectual Property Constituency (IPC) is one of the stakeholder groups and constituencies of the Generic Names Supporting Organization (GNSO) of the Internet Corporation for Assigned Names and Numbers (ICANN) charged with the responsibility of advising the ICANN Board, Organization, and other stakeholders on policy issues relating to the management of the domain name system (DNS), particularly on matter pertaining to intellectual property and consumer protection. The IPC represents the views and interests of owners of intellectual property worldwide, with a particular emphasis on trademark, copyright, and related intellectual property rights and their impact on and interaction with the DNS.

We also represent the interests and concerns of consumers who depend on strong intellectual property protections as an essential element of consumer confidence, consumer trust and consumer protection. Our members include individuals, companies, law firms, and intellectual property organizations from around the world.

While the Revised Directive on Security of Network and Information Systems (NIS2) primarily relates to network and information system security, intellectual property protection is closely intertwined with cybersecurity. IP assets are often leveraged by bad actors as vectors for security threats and other abuses, such as phishing, distribution of malware, and other similar harmful activities.[1] The IPC commends the positive progress reflected in the NIS2 draft, particularly with respect to the DNS and proposed requirements that domain name registration data be complete, true, and accurate, and that access to such data be available to facilitate legitimate third-party purposes. Access to complete, true, and accurate domain name registration data is critical for intellectual property enforcement and consumer protection, which are key components of a broad cybersecurity framework.

The European Commission expressly recognized that "access to Internet domain name registration information ('WHOIS data') is important for criminal investigations, cybersecurity and consumer protection."[2] The European Parliament has noted that approximately 75% of requests for access to domain name registration data from parties with legitimate interests remain unanswered and almost all requests that receive an answer are denied.[3] Recently, the Interisle Consulting Group found that 86.5% of domain name registrants cannot be identified while also finding that only 11.5% of domain names have been registered to natural persons and are thus subject to the European Union General Data Protection Regulation (GDPR).[4] The Council of the European Union has also expressed the importance of access to domain name registration data and noted "the concerns raised by law enforcement authorities, cybersecurity organisations and intellectual property rights holders about the negative impact of the limitations of access to WHOIS data on their work. Finding a workable solution for access to non-public WHOIS data should be treated as a matter of priority."[5]

Unfortunately, after more than two years of work, the ICANN community has not yet been successful in its efforts to develop, implement and deploy a working solution to facilitate reasonable access to complete, true, and accurate domain name registration data for legitimate purposes including those of law enforcement, cybersecurity, and intellectual property and consumer protection, following the global redaction of a substantial portion of registration data in response to the GDPR. The EU has an important opportunity to facilitate success in this area by providing additional clarity on domain name registration data processing requirements. The IPC greatly appreciates this opportunity to provide its input accordingly. Please find our specific suggested clarifications and amendments to the NIS2 draft below for your consideration.

Suggested Clarifications and Improvements

Ensure the term "DNS service provider" is adequately defined

Article 4.14 of NIS2 currently describes a DNS service provider as "an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers." Article 4 contains various other definitions of certain service providers who would likely fall within this definition of "DNS service provider" but the current NIS2 draft does not make this clear. For example, it is not clear whether the current definition of "DNS service provider" would cover any or all of the additionally specified service provider types, as described in Article 4.9, namely, "a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive…."

Given the evolution of the current domain name registration ecosystem over time, we suggest that Article 4 fully define and clarify that all entities providing domain name registration services are to be considered "DNS service providers" and that this term includes top-level domain registries as well as:

- domain name registrars
- domain name resellers
- privacy registration service providers
- proxy registration service providers

This definition should then apply consistently wherever the term "DNS service provider" is used, such as in Articles 23.1, 23.2, 23.3 and Recitals 15, 61, 62.

Accordingly, we propose the following specific amendments to Article 4.9:

Current Text	**Proposed Amendments**
Article 4.14. 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;	Article 4.14. 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers, specifically including top-level domain registry operators, domain name registrars, domain name resellers, privacy registration service providers, and proxy registration service providers;

Define what data constitutes "domain name registration data"

In several places, the draft NIS2 uses the term "complete domain name registration data". For the avoidance of doubt, we believe that the directive should explicitly define the minimum set of registration data elements as follows:

- domain name
- RDAP server name
- domain creation, update and expiry dates
- sponsoring registrar name
- all domain status information (EPP status codes)
- registrant ID number
- registrant name
- registrant organization (if any)
- registrant email address
- registrant postal address (street address, city, state/province, country, postal code)
- registrant telephone number
- name server(s) (if any)

Accordingly, we propose an amendment to Article 4, as follows, to provide this definition:

Current Text	Proposed Amendments
[N/A]	Article 4.27. 'complete domain name registration data' means the full set of mandatory data elements to be collected or generated, as appropriate, by certain DNS service providers, and at a minimum shall include the domain name, RDAP server name, domain creation, update, and expiry dates, sponsoring registrar name, all domain status information (EPP status codes), registrant ID number, registrant name, registrant organization (if any), registrant email address, registrant postal address (street address, city, state/province, country, postal code), registrant telephone number, and name server(s) (if any).

Ensure an adequate definition of "DNS abuse"

Recital 60 of the draft NIS2 discusses preventing and combating "Domain Name System abuse." NIS2 would benefit by setting forward a definition of Domain Name System abuse. The ICANN Registry Agreement clearly sets forth activities that must be prohibited in connection with the use of a domain name. Therefore, we propose that "Domain Name System abuse" be defined as "distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law." Accordingly, we propose an amendment to Article 4, as follows, to provide this definition:

Current Text	Proposed Amendments
[N/A]	Article 4.28. 'domain name system abuse' means the use of a domain name to distribute malware, abusively operate botnets, conduct phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, or counterfeiting, or otherwise using a domain name to engage in activity contrary to applicable law.

Clarify the requirements concerning the accuracy of domain name registration data

There has been much debate and lack of certainty regarding the data accuracy requirements under current Union law, including in the particular context of domain name registration data. More specifically, there must be clarity as to whether the accuracy obligation relates to recording and displaying an accurate reflection of the data provided by the registrant at face value, or whether steps must be taken to confirm the accuracy (and truth/legitimacy/functionality) of the information provided and take steps where it is inaccurate (not truthful or legitimate or functional). For example, if the registrant purposely provides false or non-functional data whether or not to stymie law enforcement investigations or other third-party uses requiring truthful/legitimate data, is this to be permitted under Union law? The present draft NIS2 (nor any other legal authority issued to date) does not answer this question unambiguously. Accordingly, we propose that NIS2 clarify that data accuracy requires that data be truthful and legitimate in order to facilitate the purposes for its processing, including collection, publication, and disclosure to third parties, and not merely a right of the data subject to provide and self-verify the accuracy of the data it provides, even if false or non-functional. We propose the following amendments to Article 23.1 accordingly:

Current Text	Proposed Amendments
Article 23.1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.	Article 23.1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data. For the avoidance of doubt, the "accuracy" of such data means that it is true, legitimate, and functional data and not merely data whose accuracy is assumed by TLD registries and the entities providing domain name registration services for the TLD even if so averred by the data subject.

Ensure that all non-personal data in domain name registration data be published; define "without undue delay" more specifically

NIS2 should also clarify that all entities providing domain name registration services should make publicly available all domain name registration data that falls outside the scope of Union data protection rules, such as non-personal data of legal persons. More specifically, where a registrant is a legal person then the data in the "Registrant" field should be made publicly available, and the publication of the legal name of the registrant should not be an actionable disclosure of personal data, even if that legal name includes the name of a natural person.

Further, any data provided in the "Registrant Organization" field should be made publicly available, and in the event this results in the publication of data in the "Registrant Organization" field that in fact includes personal data, this should not be considered an actionable disclosure, provided that steps are taken promptly, when notified by the data subject, to rectify the record and cease the disclosure of such personal data. For the avoidance of doubt, the NIS2 should clarify that "publish" in this context means made accessible to anyone in an online freely-accessible database (e.g. the Registration Data Directory Service mandated by ICANN).

We would also propose amendments to Article 23.4's use of the "without undue delay" language in addition to further clarifying the appropriate scope of data publication, discussed above, as follows:

Current Text	**Proposed Amendments**
Article 23.4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.	Article 23.4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay and in no event later than two (2) business days after the registration of a domain name, domain registration data which are not personal data. For the avoidance of doubt, all domain name registration data of legal persons shall be published, as such data is beyond the scope of Union data protection rules. In the event that such data of legal persons contains personal data, publication by the data processor shall not be considered an actionable data breach, provided that steps are taken promptly, when notified by the data subject, to rectify the record and cease the publication of such personal data. "Publish" in this context shall mean made accessible to anyone in an online freely-accessible query-able database.

Establish that certain requests for disclosure of domain registration data are justified and in compliance with Union data protection law

NIS2 Article 23.5 mandates that access be provided to domain name registration data "upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law." We suggest that language be added to this article to clarify that requests relating to addressing DNS abuse or requests to facilitate the establishment, exercise or defence of legal claims be explicitly identified as categories of lawful and duly justified requests that comply with Union data protection law. We also recommend that this article include a more specific disclosure timeline requirement, similar to the proposed amendment above regarding Article 23.4. More specifically, we would propose the following amendments to Article 23.5:

Current Text	**Proposed Amendments**
Article 23.5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	Article 23.5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Well-founded requests relating to addressing DNS abuse and requests to facilitate the establishment, exercise or defence of legal claims shall be considered lawful, justified, and legitimate. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access, and in no event later than five (5) business days following the request. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Establish that publication of certain domain name registration data elements is in the public interest

Given the current lack of access to domain name registration data combined with the increasing levels of cyber threats and online illegal activity of all kinds, the NIS2 should establish that there is a public interest in the publication and disclosure of certain domain name registration data for certain legitimate purposes, and mandate that, at a minimum, the registrant organization (if any), state/province, country and a verified registrant email address be publicly available for all domain names regardless of the status of the registrant as a natural or legal person. Establishing the public interest nature of domain name registration data is equivalent to similar publicly accessible directories, including the European Trademark Register. Indeed, the public interest in the specified domain name registration data elements are of greater importance to ensuring public welfare, safety and cybersecurity than the data in the Trademark Register, in our view.

Accordingly, we suggest that a new sub-paragraph of Article 23 be added that explicitly requires the registrant organization (if any), state/province, country, and verified email address always be publicly available to ensure appropriate transparency and accountability of domain name registrants. We propose the following possible text in this regard:

Current Text	**Proposed Amendments**
[N/A]	Article 23.6. Member States shall recognize a specific public interest in the processing of domain name registration data and ensure that for all domain names the registrant's organization (if any), state/province, country, and verified email address are publicly available in order to ensure appropriate transparency and accountability of domain name registrants.

Conclusion

Once again, the IPC greatly appreciates this opportunity to provide comments regarding the NIS2 proposal. We strongly support the initiative to modernize Union law on the critical issues of network and information system security, given the ubiquity of these systems, their primacy in global connectivity and commerce, and the role they play in the daily lives of consumers and citizens in the Union and around the world. The NIS2 makes very positive strides and we hope that our input will add an important perspective leading to the enhancement of the proposal in underscoring the interrelation between intellectual property and consumer protection issues and cybersecurity. We look forward to continuing to engage on these important issues.

Respectfully submitted,

Dean Marks

IPC Vice President, on behalf of the IPC

---

[1] See, e.g., Anti-Phishing Working Group, Phishing Activity Trends Report Q4 2020 (Feb,. 9, 2021), available at https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf; F5 Labs, 2020 Phishing and Fraud Report (Nov. 11, 2020), available at https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf; SecurityTrails, Domain Security & Solutions Part 2: Phishing & Trademark Infringement Attacks (July 30, 2019), available at https://securitytrails.com/blog/domain-security-part-02-phishing-trademark-attacks; Janveva et al, Whitehall Report 4-20: Taking the Profit out of Intellectual Property Crime: Piracy and Organized Crime, Royal United Services Institute for Defence and Security Studies (March 2021), available at https://rusi.org/sites/default/files/whr_ip_crime_web_version.pdf.

[2] European Commission, Communication on the EU Security Union Strategy (24 July 2020), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN.

[3] European Parliament, Parliamentary Questions: Subject: Lack of access to WHOIS internet domain registration data (11 Feb. 2020), *available at* https://www.europarl.europa.eu/doceo/document/E-9-2020-000826_EN.html.

[4] Interisle Consulting Group, WHOIS Contact Data Availability and Registrant Classification Study (25 Jan. 2021), available at http://www.interisle.net/ContactStudy2021.html.

[5] Council of the European Union, Memorandum from the General Secretariat of the Council to the Permanent Representatives Committee re EU Lines To Take on WHOIS policy reform (23 Oct. 2018), available at https://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf.