Petillion
Attorneys - Advocaten - Avocats

Flip Petillion
fpetillion@petillion.law
+32 484 652 653

Friday, May 11, 2018

EU Commission
Article 29 Working Party
All heads of DPAs

Cc:
Vice President Jyrki Katainen, European Commission (Jobs, Growth, Investment and Competitiveness)
European Commissioner Elżbieta Bieńkowska (Growth)
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Vice President Andrus Ansip, European Commission (Digital Single Market)
European Commissioner Mariya Gabriel (Digital Economy and Society)
Directorate-General for Communications Networks, Content and Technology

European Commissioner Věra Jourová (Justice, Consumers and Gender Equality)
Head of Unit Mr. Bruno Gencarelli (Data Protection)
Directorate-General for Justice and Consumers

Deputy Head of Unit Ms. Cathrin Bauer-Bulst (Cybercrime)
Directorate-General for Migration and Home Affairs

Re: GDPR and WHOIS: Impact on law enforcement, IP rights and consumer protection – Digital economy

Dear Madam,
Dear Sir,

I am writing you to propose some effective solutions for the problems raised by the need to implement the EU General Data Protection Regulation 2016/679 (GDPR) and its impact on the availability of WHOIS data of domain names.

Due to time constraints and uncertainty regarding their obligations under the GDPR, ICANN[1], domain name registry operators and registrars risk taking actions which will have a detrimental impact on certain essential functions of the Internet, and which will impair crucial principles and considerations

[1] The Internet Corporation for Assigned Names and Numbers is the entity responsible for the stable and secure operation of the Internet and its domain name system (DNS).

laying at the basis of EU law, such as proportionality with other fundamental rights, transparency, and accountability.

In view of the way the WHOIS and GDPR debate has been developing over the past months, I believe I should share my experience on the subject. Through the work that I have done over the past twenty-five years as a lawyer engaged in the fields of privacy, intellectual property and information technology, in my practice and through my active memberships in international organisations, I have been a privileged witness of the essential role of WHOIS data in the fight against cybercrime, counterfeiting, and cybersquatting.

There are reasons to limit unrestrained access to WHOIS data to protect specific personal information falling under the GDPR's scope. However, one would expect that the GDPR's implementation remains in balance with other regulatory frameworks also implemented by the European institutions, such as those meant to protect consumers, to prevent fraud and money laundering, to enforce intellectual property rights, etc.

As a result, it is important that (i) both single query and automated access to certain essential WHOIS data are maintained, and (ii) a continued dialogue and guidance is upheld until the adoption of a compliant WHOIS model which balances the rights and legitimate interests of all stakeholders involved.

1. The WHOIS system is indispensable for our society and the digital single market

For nearly twenty years, WHOIS data have been generally available to the public. Interested third parties may use single query access to WHOIS data to identify and contact the registered domain name holder (the registrant). Expedient access to accurate WHOIS data is vital to law enforcement authorities, consumers, intellectual property owners and cybersecurity service providers.

Access to WHOIS data allows law enforcement authorities to rapidly find connections between different domain names which may otherwise go unnoticed. These connections may assist in uncovering terrorist networks, cybercrime, fraud, money laundering, etc. Consumer protection organisations and cybersecurity service providers also depend on (automated) access to WHOIS data to safeguard consumer trust and secure critical networks. Consumers may query WHOIS data to verify the Uniform Resource Locator (URL) resolution to a website. Intellectual property owners depend on WHOIS data in their continuous battle against online infringers. The information is used to identify owners of websites who are hosting illegal content, selling counterfeit products or have otherwise engaged in abusive domain name registration.

2. Specific WHOIS purposes and GDPR

Below are examples of legitimate WHOIS purposes and the legal basis justifying the lawful disclosure of essential WHOIS data elements. The list of examples is not exhaustive.[2]

a) Purpose 1: To investigate fraud and verify the legitimacy of invoices and other communications

All internet users, including consumers, businesses, rights holders and law enforcement agencies depend on publicly accessible WHOIS information to quickly verify whether a particular invoice sent via email is legitimate. By querying the WHOIS information of the domain name related to the email address, recipients can verify whether the holder of the domain name is the natural or legal person mentioned on the invoice. There is no alternative way to perform this test.

The relevant and necessary data elements for this legitimate purpose are the registrant's **name and email address**. A name is required to verify whether the identity of the sender corresponds to the identity claimed in the communication. An email address allows to verify whether the email address is related to other communications received by the sender and to quickly contact the registrant to obtain further information.

Given the substantial public interest of all Internet users to combat fraud and illegal activity on the Internet and beyond, the need for the public disclosure of the name and email address of the registrant of a domain name is based on **article 6 (f) GDPR**[3].

This legal basis requires balancing the public interests involved against the fundamental rights and freedom of the registrant. As the purpose is limited to identifying and potentially contacting the registrant, the invasiveness of the disclosed data elements and the impact on the registrant are limited, especially in relation to the overwhelming public interests involved. A registrant always retains the ability to register a domain name with an unidentifiable email address (example: info@organisation.com). There are numerous free email address providers available and a registrant may even opt to use a privacy or proxy service when registering the domain name. Additionally, at the registration of a domain name, a registrant is (and can always be) sufficiently informed about the publication and possible further use of essential personal information. In this regard, the data subject will have reasonable expectations that this information will be accessible in relation to the registered

[2] WHOIS data serves many legitimate purposes, many of which may warrant the processing of more WHOIS data elements than determined in the examples provided. For example, the use of public WHOIS data for law enforcement purposes allows the effective investigation of and action against serious crime, terrorism, fraud, consumer deception and other violations of law. To tackle large-scale cyber-criminality, automated access to so-called 'thick' WHOIS information (both current and historic) is often vital. Thick WHOIS provides for the registrant's contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status information supplied by a thin registry.

[3] "*Processing shall be lawful only if and to the extent that at least one of the following applies: … (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

domain name. Because this purpose concerns all Internet users and immediate access is often essential, public disclosure of the registrant's name and email address is warranted.

As a result, the availability of the registrant's name and email address in a public WHOIS system must be maintained for the purpose of investigating online fraud and because of prevailing public interests, accountability and transparency considerations.

b) Purpose 2: To contact a registrant about possible infringements

The disclosure of a registrant's **email address** in a public WHOIS system is essential for the legitimate purpose of expeditiously contacting the registrant in case of possible infringements.

Generally, when rightsholders become aware of a website or online activity possibly infringing their intellectual property, commercial or other right, they will first attempt to contact the owner of the website concerned before taking any legal action. For this, they need a rapid and effective way of communication. An email address is also essential to immediately send a cease and desist letter to prevent further substantial damages.

The legal basis of **article 6 (f) GDPR** and the corresponding balancing exercise favour the rights and interests of several third parties, including commercial entities and intellectual property rightsholders. The publication of the email address has a limited impact on the registrant. As provided above, a registrant always retains the possibility to use an unidentifiable email address. The risk for the registrant receiving unsolicited emails cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Masking the email address of registrants unduly restricts the protection of consumers, and enforcement of intellectual property and commercial rights and prevents parties from amicably settling disputes related to potential online infringements.

As a result, the availability of the registrant's email address in a public WHOIS system must be maintained for the purpose of contacting the registrant about possible infringements and because of the prevailing interest of third parties, as well as accountability and transparency considerations.

c) Purpose 3: To serve a writ with and initiate legal proceedings against an infringing registrant

To rapidly examine whether legal action is possible on the basis of jurisdiction and applicable law, a rightsholder needs access to information regarding the registrant's **state and/or country**. National courts will only start proceedings when the claimant produces evidence that the writ of summons was served with the defendant. As a result, a rightsholder can only initiate legal proceedings if he or she knows the **name and postal address** of the defendant.

In the case of online infringements, such as on websites hosting illegal content, selling counterfeit goods or misleading consumers, the infringer is generally not known. WHOIS information will be the only way to obtain the name and postal address of the infringer and initiate legal proceedings. If this information is inaccessible or dependent upon a discretionary disclosure decision by a registrar or registry, the accountability of website operators would be severely reduced.

One may argue that the balancing exercise of **article 6 (f) GDPR** favours not to make the postal address of every natural person registrant publicly available. However, given the strong public interest and the fundamental right to an effective remedy and the protection of consumers and intellectual property rights, effective access to a registrant's postal address should be maintained. A WHOIS system should take into account the rights and interests of the public and third parties.

As a result, the WHOIS system must maintain the information necessary to analyse the jurisdictional basis and applicable law for a legal claim publicly accessible, such as the registrant's state and/or country. Effective access to a registrant's full postal address should further be maintained until a less intrusive WHOIS system is implemented which takes into account the rights and interest of the public and third parties.

d) Purpose 4: To identify a registrant in UDRP proceedings and to prevent 'cyberflight'

Rightsholders depend on administrative proceedings, such as the Uniform Domain-Name Dispute-Resolution Policy (UDRP), to efficiently tackle abusive domain name registrations such as cybersquatting. The proper functioning of these administrative proceedings entirely depends on accessible WHOIS data elements. A complainant needs a registrant's **name, email address and location** to properly file a complaint and acquire the suspension, cancellation or transfer of the infringing domain name.

The registrant's **name** is necessary to identify the infringer and show, for example, that the registrant has no rights or legitimate interests in the domain name, that he or she was not authorised to register the domain name and that he or she registered and used the domain name in bad faith. A rightsholder requires the registrant's **name and email address** to investigate whether he or she has engaged in a pattern of bad faith registrations, using automated WHOIS access. A rightsholder cannot determine the language of the UDRP complaint and cannot argue whether the registrant was aware of the rightsholder rights if he or she has no access to WHOIS information regarding the registrant's **location**, including his country, state and/or city.

The effective functioning of the UDRP system serves several legitimate interests pursuant to **article 6 (f) GDPR.** The inability to tackle abusive domain name registrations through UDRP would result in a proliferation of cybersquatting, counterfeiting and phishing, which would not only severely damage rightsholders, but also consumers.

The expeditious identification of an infringer is further necessary to prevent 'cyberflight'. An infringer can easily avoid or severely delay administrative or judicial proceedings when there is no access to current and historic WHOIS data. The infringer can simply transfer, change or cancel his domain name registration after learning of a potential action. The initiation of UDRP proceedings allows the domain name registration to be 'locked', preventing any changes to the registration and eliminating chances of 'cyberflight'. Without expedient access to WHOIS data, cyberflight cannot be avoided.

As a result, the strong public interest in maintaining an effective UDRP system and the fundamental right to an effective remedy and the protection of consumers and intellectual property rights, warrant

effective access to a registrant's name, email address and location. This access should at least be maintained until a WHOIS system is implemented that takes into account the rights and interests of the public and third parties.

e) Conclusion

The WHOIS system fulfils several legitimate purposes which are essential for the proper functioning of the Internet, the protection of consumers, the enforcement of intellectual property and law enforcement. For several of these purposes, article 6 (f) of the GDPR warrants that at least the name and email address of the registrant remain publicly available in favour of public or third-party interests. For other purposes, it is essential that important WHOIS data, such as the registrant's postal address, remain readily accessible until a less intrusive WHOIS system is effectively implemented.

In addition, the requirement to publish WHOIS data is comparable and serves a similar purpose to the disclosure requirement for companies in a central, commercial or companies register imposed on EU Member States and for trademark applicants and holders in international, European and national trademark registers.[4] In this regard, the Court of Justice of the EU has specifically determined that the need to protect the public interest and the legitimate interests of third parties takes precedence over an individual's right to data protection when publishing a limited number of personal data items in a public register.[5]

3. The proposed interim WHOIS model risks unnecessary over-complying with the GDPR and cannot be implemented in time

ICANN's discussions on updating the existing WHOIS system have not yet led to a final outcome and, therefore, ICANN and its stakeholders have started the development of an interim model to ensure GDPR compliance, pending a final update of the WHOIS system.[6]

The proposed interim model was published by ICANN on February 28, 2018 and aims to establish tiered access to WHOIS data by means of a formal accreditation program.[7] The model abolishes automated WHOIS access and significantly limits single query access for parties not formally accredited under the program. Consequently, these parties will depend on the disclosure decision of the relevant registry and/or registrar.

---

[4] See Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, *OJ* L 169, 30.6.2017, p. 46–127; article 44 Regulation 2017/1001 Of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, *OJ* L154.

[5] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni,* Court of Justice of the European Union (Second Chamber), 9 March 2017, C-398/15, ECLI:EU:C:2017:197.

[6] The process of updating ICANN's WHOIS policies already began in November 2012, and thus, well before the adoption of the GDPR by the European Parliament in April 2016. The introduction of the GDPR made the focus of the debate shift towards ensuring GPDR compliance.

[7] Proposed Interim Model for GDPR Compliance - Summary Description, ICANN Org, 28 February 2008, https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf. See also https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf for a more extensive document on the proposed interim compliance model (The "Cookbook"), published by ICANN Org on 8 March, 2018.

The proposed interim model does not correspond with ICANN's principal objective of achieving compliance with its obligations under the GDPR while maintaining the existing WHOIS system to the greatest extent possible. Indeed, the proposed interim model risks over-correcting the balance in favour of privacy interests, to the detriment of other vital public and third-party interests. For example, the omission of certain identification and contact information from the public WHOIS records, notably the registrant's name and email address, critically impairs the ability to expeditiously identify and contact the registrant.

The proposed interim model also does not correspond with the GDPR's intended purposes. In its fourth recital, the GDPR provides:

> "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

The principle of proportionality requires that the measures taken to protect the privacy and data of natural persons are necessary and adopted in the least onerous way and balanced with the competing interests of the public and third parties. These rights include the freedom and access of information, the right to an effective remedy, the right to conduct a business and the right to intellectual property. The proposed interim model would unduly restrict the exercise of those other rights and damage the interests of third-parties. It is therefore not proportional.

In addition, as the GDPR implementation deadline is approaching, it will be impossible to implement the proposed interim model in time. It cannot be anticipated that, in less than 15 days, registries and registrars update the core architecture of their complex technical networks.

In the absence of clear guidance and a set of standards and processes, it is uncertain how various registries and registrars will collect, and make available, WHOIS data once the GDPR's deadline for implementation has lapsed. Different approaches towards the GDPR's implementation may lead to a fragmented WHOIS system and a potential 'blackout'. As a result, crucial information risks becoming unavailable to law enforcement and interested third parties for an indeterminate period of time.

4. Solutions

The lack of protection of certain personal information during a brief period of time is no reason to rush into adapting the WHOIS system without a fully operational alternative that ensures access to essential WHOIS data by third parties with a legitimate interest to access such data. While the existing WHOIS system has been the subject of the European data protection regulatory framework for more than 20 years, no action has been considered previously.

Therefore, to ensure the maintenance of a stable WHOIS system and the protection of essential public interests, the EU authorities should maintain an ongoing dialogue with ICANN, its stakeholder, the registries and registrars.

In the interim, the EU Commission, the article 29 Working Party and the national DPAs have all interest in requiring ICANN, its registries and registrars to keep essential WHOIS data readily available. They should provide clear guidance aimed at implementing a balanced WHOIS model and prevent over-compliance with the GDPR. This approach will favour essential public and legitimate third-party interests.

5. Action Points

As explained earlier, I strongly encourage the European authorities, including the EU Commission, the article 29 Working Party and the national DPAs, to:

1. Maintain an ongoing dialogue with ICANN, its stakeholders, registries and registrars in relation to the publication of personal data in the public WHOIS system until a stable and acceptable compliance model can be adequately implemented; and

2. Cooperate with all stakeholders in developing a GDPR-compliant and balanced WHOIS model, specifically providing clear guidance to keep essential information, such as the registrant's name and email address, readily available, in accordance with public and legitimate third-party interests.

I thank you for your consideration of this important issue and remain at your disposal to further discuss practical solutions.

Yours sincerely,

Flip Petillion