European Communities Trade Mark Association

23 May 2018

ECTA POSITION PAPER ON WHOIS

I. INTRODUCTION

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "GDPR") takes effect on 25 May 2018.

Over the past several months, there were intense discussions on the impact of the GDPR to personal data that participants in the generic Top-Level Domains (gTLDs) domain name system collect, display and process (including registries and registrars) pursuant to Internet Corporation for Assigned Names and Numbers ("ICANN"), contracts and policies.

On 28 February 2018, ICANN has released "the Proposed Interim Model for GDPR Compliance – Summary Description" (hereafter the "Proposed Interim Model")[1] and on 8 March 2018, "the Interim Model for Compliance with ICANN Agreement and Policies in relation to the European Union's General Data Protection Regulation – Working Draft for Continued Discussions" (hereafter the "Interim Compliance Model")[2], draft which is currently under discussions.

To comply with the GDPR, ICANN envisages a shift from the current requirement for gTLD registries and registrars to provide open, publicly available to registration directory services (hereinafter the "WHOIS") to an approach requiring a layered/tiered access model for the WHOIS.

An accreditation program for access the WHOIS data is currently under discussion as well as which elements of the WHOIS data should only be available to accredited users.

WHOIS data are part of everyday life for an intellectual property holder. Such data are used in conducting trade mark enforcement investigations, for sending cease and desist letters, for communicating with the registrants, for preparing and prosecuting UDRP / URS complaints, and in general to protect the interests of intellectual property owners, of consumers as well as law enforcement authorities in order to try to keep the Internet safe from security breaches and other nefarious/criminal behavior.

Bad actors operate at a global scale, across multiple registrars and top-level domains, sometimes using thousands of names in coordinated and automated attacks. Harms range from consumer fraud, disinformation, spam, phishing, botnet attacks, and distributed denial of service (DDOS) attacks to the more grim, including human trafficking and child abuse.

[1] https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance

[2] https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf; https://www.icann.org/resources/files/1213969-2018-03-08-en.

WHOIS data elements are useful in preventing or in investigating and prosecuting against these harms.

However, under the ICANN's current proposed model public access to the WHOIS data elements critical to multiple functions within the DNS will be severely restricted.

If adopted, such a restriction will impact the interests of the intellectual property owners, of consumers as well as the safety of the Internet.

The Interim Compliance Model as released on 8 March 2018 may be updated as conversations with the community and data protection authorities progress. The same applies also for the accreditation program.

II. COMMENTS

A. The Interim Model for Compliance

Among the aspects presented within the draft of Interim Model for Compliance released on 8 March 2018, we highlight some of the points which will have an impact for the enforcement if intellectual property rights, namely:

1. **The restrictions to access WHOIS data should be differentiated between natural and legal persons domain name registrations**

   Although the GDPR provisions apply to the processing of personal data which is clearly defined as any information relating to an identified or identifiable natural person, the data subject[3], the Interim Compliance Model provides that such will apply to all domain name registration data that is contained in the WHOIS system, without differentiating between the registrations of legal and natural persons.

   In our view, it is necessary to draw a distinction between natural and legal persons domain name registration.

   The goal should be to preserve access to the public information from WHOIS to the greatest extent possible and not to go beyond the purpose of the GDPR.

   Several European ccTLD registry operators, such as EURid and DNS Belgium, already make a clear distinction between natural persons and legal entities, based on self-certification. When a registrant does not identify itself as a natural person, all registration information remains publicly accessible.

   Thus, in our view, to the extent that the registrations of the domain names will not reflect personal data within the meaning of the GDPR, such data should be publicly accessible, and in case individual's personal data are involved in relation to the registration of a domain name for a legal person, an opt in system, for example, could be implemented or another solution should be found in order to allow public access to WHOIS data of legal entities.

[3] Art. 4(1) GDPR

2. Public WHOIS

Under the current system, registries and registrars are required to operate WHOIS providing free public query-based access to up-to-date data concerning active domain name registrations.[4]

However, the public access to WHOIS data as we know it will not continue after 25 May 2018.

ICANN proposal of access to WHOIS data was a layered tiered access to these data.

The Interim Compliance Model provides what data elements will continue to be published in the public layer of WHOIS, namely:

(i) The **registrant "name"** field will not be published in the public WHOIS. However, the registrant "organization" would be required to be published (if applicable) so that registrations of legal entities would readily include the name of the entity;

(ii) The **registrant's state/province and country will be published**, but the address fields that could be used to more specifically identify the registrant would not be included in the public WHOIS (e.g. street, city, postal code). This would enable non-accredited users to determine the registrant's general location and likely jurisdiction, but would generally not enable identification of the registrant;

(iii) The public WHOIS will include **an anonymized email address or a web form from which messages could be forwarded to the registrant email address**. This approach will enable non-accredited users to contact, but not identify, the registrant[5];

(iv) The **registrant phone and fax would not be required to be published in the public WHOIS**;

(v) Similar to the registrant email field, the public WHOIS will include **anonymized email addresses or a web form from which messages could be forwarded to the administrative and technical contact email addresses**. No other contact details of the administrative and technical contacts would be published in the public WHOIS.

A sample of a Minimum WHOIS Output Fields is provided herein below:

[4] Registry Agreement, Specification 4; Registrar Accreditation Agreement, Registration Data Directory Service (WHOIS) Specification

[5] Considering that anonymized email addresses rarely work, it might be envisaged to be provided for domain names to be suspended by registrars when un-anonymized email address return an undeliverable receipt in order not to burdensome more the intellectual property owners.

WHOIS Data Fields	ICANN Interim Compliance Model Legal and Natural persons
Domain Name	Display
Registry Domain ID	Display
Registrar WHOIS Server	Display
Registrar URL	Display
Updated Date	Display
Creation Date	Display
Registry Expiry Data	Display
Registrar Registration Expiration Date	Display
Registrar	Display
Registrar IANA ID	Display
Registrar Abuse Contact Email	Display
Registrar Abuse Contact Phone	Display
Reseller	Display
Domain Status	Display
Domain Status	Display
Domain Status	Display
Registry Registrant ID	Do not display
Registrant Name	Do not display
Registrant Organization	Display
Registrant Street	Do not display
Registrant City	Do not display
Registrant State/Province	Display
Registrant Postal Code	Do not display
Registrant Country	Display
Registrant Phone	Do not display
Registrant Phone Ext	Do not display
Registrant Fax	Do not display
Registrant Fax Ext	Do not display
Registrant Email	Anonymized email or web form
Registry Admin ID	Do not display
Admin Name	Do not display
Admin Organization	Do not display
Admin Street	Do not display
Admin City	Do not display
Admin State/Province	Do not display
Admin Postal Code	Do not display
Admin Country	Do not display

WHOIS Data Fields	ICANN Interim Compliance Model Legal and Natural persons
Admin Phone	Do not display
Admin Phone Ext	Do not display
Admin Fax	Do not display
Admin Fax Ext	Do not display
Admin Email	Anonymized email or web form
Registry Tech ID	Do not display
Tech Name	Do not display
Tech Organization	Do not display
Tech Street	Do not display
Tech City	Do not display
Tech State/Province	Do not display
Tech Postal Code	Do not display
Tech Country	Do not display
Tech Phone	Do not display
Tech Phone Ext	Do not display
Tech Fax	Do not display
Tech Fax Ext	Do not display
Tech Email	Anonymized email or web form
Name Server	Display
Name Server	Display
DNSSEC	Display
DNSSEC	Display
URL of ICANN Whois Inaccuracy Complaint Form	Display
>>> Last update of WHOIS database	Display

The GDPR expressly provides that the right to the protection of personal data is not an absolute right. It must be considered in relation to its function in the society and be balanced against other fundamental rights, such as the right to the protection of intellectual property and to an effective remedy, in accordance with the principle of proportionality.

In our view, ICANN should reconsider the proposal to hide the registrant email address from the WHOIS public accessible data as this is not proportionate in view of the significant negative impact on law enforcement, consumer protection, cybersecurity and rights protection. A registrant's email address is vital as an - if not the most – important data point for rapidly contacting the registrant for the purposes of cybercrime investigations, intellectual property enforcement, the analysis of patterns of malicious registrations, counterfeiting, etc.

3. Access to Non- Public WHOIS data - Accreditation program

ICANN identified the following possible approaches for providing access to the full WHOIS data to third-party requesters:

1) a self-certification approach where certain third-parties identify their legitimate purpose for access to the data and agree to use the data for the identified limited purpose,

2) a certification approach where certain third-parties identify their legitimate purpose for access to the data and agree to use the data for the identified limited purpose and in compliance with an approved code of conduct,

3) an accreditation approach where a defined set of third-party requesters are certified under an accreditation program have access to the data after being accredited/certified, and

4) a legal due process approach where access is only granted when required by applicable law, such as when the third-party requestor provides a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction.

The Interim Compliance Model provides that registries and registrars allow access to non-public registration data only for a defined set of third-party requestors certified under a formal ICANN-managed accreditation program.

Under this approach, user groups with a legitimate interest and who are bound to abide by adequate measures of protection, for example law enforcement agencies and intellectual property lawyers, could access non-public WHOIS data based on pre-defined criteria and limitations under the formal accreditation program.

With respect to the accreditation program, ICANN had meetings with EU data protection authorities in order to receive guidance on the proposed accreditation program.

Article 29 Data Protection Working Party ("WP29") has on 11 April 2018 issued a letter to ICANN[6] with respect to WHOIS and the GDPR.

WP29 welcomed the decision of ICANN to propose an interim model which involves layered access, as well as an "accreditation program" for access to the non-public WHOIS data as well as the proposal to introduce alternative methods to contact registrants or administrative and technical contacts, without public disclosure of registrants' personal email addresses (referred to as "anonymized email, web form, or other technical means").

However, several concerns have been expressed by WP29 with respect to several aspects of the Interim Compliance Model.

[6] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf

A proposed accreditation model to ensure continued WHOIS availability for eligible entities seeking data access[7] is currently under discussions at ICANN level and continues to be refined.

Should an accreditation and access model not be agreed upon in the next few weeks, WHOIS data will be gated by ICANN and thus WHOIS will "go dark" on 25 May 2018.

Such a development would disable a critical tool employed for the safe and stable operation of the DNS, the prevention of crime, the conduct of vital cybersecurity operations, the protection of consumers, and the enforcement of intellectual property rights.

By ICANN's own estimation so far, a model might not be implemented until at least December 2018 or even longer. Also, some contracted parties might decide to deviate from the model if this would be necessary in order to mitigate their GDPR enforcement risks.

The proposed accreditation model provides several categories of access.

For what interests the IP owners and their representatives, the provisions read on 27 April 2018 as follows:

This category is designed for intellectual property rights holders, including trade mark, patent or copyright owners or their agents (agents may include legal representatives, trade associations, data aggregators and brand protection companies) who need to investigate and enforce their intellectual property rights. It also may apply to OpSec actors who address brand-based phishing that facilitates criminal theft, product counterfeiting, etc. Applicants in this category may also include members in good standing of a national or state/provincial licensing organization (such as a bar association, or a patent and trade mark office), or of a related trade association.

Legitimate and lawful purposes for access include:

- *Investigating, tracking and preventing intellectual property infringement*
- *Researching and investigating intellectual property infringement trends*
- *Contacting infringing parties and relevant service providers*
- *Identifying domains to support IP enforcement*
- *Initiating or facilitating administrative proceedings*
- *Maintaining intellectual property rights*

[7] http://www.ipconstituency.org/accreditation; http://www.ipconstituency.org/assets/Outreach/Annotated%20-%20WHOIS%20Accreditation%20and%20Access%20Model%20v1.4.pdf; Comments to-date are archived here: https://mm.icann.org/pipermail/accred-model/2018-April/date.html. The main comment email address is gdpr@icann.org. The comments of the Non-Commercial Stakeholders Group on the Draft IPC/BC Purpose Statement Published on 27 March 2018 can be found at: https://www.icann.org/en/system/files/files/gdpr-comments-ncsg-accreditation-access-non-public-whois-data-09apr18-en.pdf

Examples of investigation and enforcement activity include:

● *Prevention of consumer confusion, theft and fraud and other crimes (e.g. counterfeiting) through infringement of trade marks*
● *Preventing the unauthorized distribution of copyrighted material*
● *Responding to trade mark related claims*
● *Trade mark clearance*
● *IP evaluation and investigation*

The application template for applicants in this category includes:

● *Identity of the applicant*
● *Contact information*
● *Standing for application (organizational mission)*
● *Evidence of organizational formation or incorporation*
● *Statement regarding intended use of data*

This category of user must also agree to follow vetting and accreditation processes described in the accreditation model. The one available on April 27th, 2018 is the following - http://www.ipconstituency.org/assets/Outreach/Annotated%20-%20WHOIS%20Accreditation%20and%20Access%20Model%20v1.4.pdf.

Conclusion: ICANN should put in place a provisional mechanism for accessing any non-public data from the WHOIS for users with a legitimate purpose until the interim WHOIS model and the accompanying accreditation system is fully operational on a mandatory basis for all contracted parties.

4. **An urgent solution has to be found for the continuation of functioning of the UDRP / URS system until the accreditation program is put in place**

The black out of the WHOIS will affect the functioning of the UDRP / URS system as well.

We mention herein below some elements from the UDRP / URS system which will be affected:

a. **UDRP/URS**

- Registrant has registered the domain name in order to prevent the trade mark holder or service mark from reflecting the mark in a corresponding domain name, provided that Registrant has engaged in a pattern of such conduct (a pattern can't be shown if there is no access to searchable data);

- Registrant registered the domain name primarily for the purpose of disrupting the business of a competitor (can't be shown that the domain name was registered by a competitor if no data are available as to who registered it);

- Possibility that providers cannot serve the UDRP/URS complaint if an email address cannot be obtained;

- Possibility that the language of the URS proceeding cannot be determined;
- Possibility that the URS provider cannot translate the notice of URS complaint into the predominant language used in the Registrant's country or territory;
- Possibility that URS complainants cannot know the language of a possible response;
- Possibility that URS complainants do not know whether the URS complaint was translated into the correct language(s) and that proceedings were administered correctly.

b. UDRP Element 2:

- It cannot be argued that the registrant is not commonly known by the domain name at issue;
- It cannot be determined if the registrant has been authorized by the trade mark holder;
- It cannot be determined if the registrant is an authorized reseller of the trade mark holder's product;
- It cannot be determined on what date the domain name was "registered" by the current domain name holder if it was transferred to this current domain name holder (it requires being able to see the WHOIS history).

c. UDRP Element 3:

- It cannot be determined if registrant has engaged in a pattern of bad faith registrations, Rule 4(b)(ii);
- It cannot be determined if the registrant is in a particular geographic region to be able to argue that the registrant knew or should have known of the trade mark being asserted;
- It cannot be determined if the registrant is technically a "competitor" that has registered the domain name for the purpose of disrupting the business of the complainant, Rule 4(b)(iii).

Conclusion: ICANN should focus on how to maintain the operation of the UDRP / URS, keeping available essential information to IP owners and accredited dispute resolution providers as an urgent matter after 25 May 2018, considering the implications of the envisaged changes regarding the access to WHOIS data.

If no viable solution is found in order to maintain operational the WHOIS, then, at least the second element of the UDRP/URS should be transformed in order for the burden to prove legitimate rights or

interest in a domain name to shift to the respondent. This would allow brand owners to claim rights under the first element and provide evidence of bad faith registration and use, where possible. The respondent would have to show legitimate rights or interests in the disputed domain name. Today the burden shifts in most cases once the complainant shows a prima facie case. Since the elements which are needed to show this prima facie cases would be gated and would reside in the control of the respondent, the changing in the burden a priori may assist brand owners to tackle cybersquatting when the identity of the respondent is unknown. However, the above will not solve the problems triggered under the Rules 4(b)(ii) or (iii) of the UDRP/URS.

III. CONCLUSIONS

WHOIS as we know it will cease to exist starting from 25 May 2018, and might be the subject to a non-determined period of blackout.

ECTA through the voice of its association and of its members:

1. is asking the European Data Protection authorities to give as much guidance as possible as to what DPAs would allow in terms of data publication through the WHOIS;

2. is asking ICANN to ensure an interim mechanism for access to any non-public data before any data is put behind a gate;

3. is committed to working together with the IPC and BC to develop an interim accreditation model accommodating the rights and interests of intellectual property rights holders;

4. is advocating to ICANN the retention of the current WHOIS system to the greatest extent possible while ensuring compliance with the GDPR.

***

ECTA, which was formed in 1980, is an organisation concerned primarily with trade marks and designs. ECTA has approximately 1,500 members, coming from all the Member States of the EU, with associate Members from more than 50 other countries throughout the world. ECTA brings together those practicing in the field of IP, in particular, trade marks, designs, geographical indications, copyright and related matters. These professionals are lawyers, trade mark and patent attorneys, in-house lawyers concerned with IP matters, and other specialists in these fields. ECTA does not have any direct or indirect links to, and is not funded by, any section of the tobacco industry.

The extensive work carried out by the Association, following the above guidelines, combined with the high degree of professionalism and recognised technical capabilities of its members, has established ECTA at the highest level and has allowed the Association to achieve the status of a recognised expert spokesman on all questions related to the protection and use of trade marks, designs and domain names in and throughout the European Union, and for example, in the following areas:

- Harmonization of the national laws of the EU member countries;
- European Union Trade Mark Regulation and Directive;
- Community Design Regulation and Directive;
- Organisation and practice of the EUIPO.

In addition to having close links with the European Commission and the European Union Intellectual Property Office (EUIPO), ECTA is recognised by WIPO as a non-Government Organisation (NGO).

ECTA does also take into consideration all questions arising from the new framework affecting trade marks, including the globalization of markets, the explosion of the Internet and the changes in the world economy.