OPERATING IN THE POST-GDPR LANDSCAPE

Investigating and tackling online IP infringements

Petillion

Petillion

The highly anticipated EU General Data Protection Regulation (GDPR) came into effect on 25 May. While this was certainly not the day of judgment for companies and organisations handling personal data, it carried some major implications for entities depending on essential information to protect their interests.

In our previous practice guide 'WHOIS behind GDPR?', we discussed the issue of over-compliance with the GDPR due to uncertainties, misrepresentations and the fear of high fines. We examined how over-extensive compliance efforts made it considerably harder for businesses to enforce their IP and commercial rights because access to essential information in the Internet's WHOIS system was no longer readily accessible.

This guide aims to provide rightsholders with practical insight and solutions on how to investigate online IP infringements and enforce their rights in the post-GDPR landscape without expeditious access to essential WHOIS information. We also determine essential positions and actions points to ensure the effectiveness of IP protection online.

Content

A.	WHOIS POST-GDPR	3
B.	PLAYERS IN DOMAIN NAME REGISTRATION	5
C.	INVESTIGATING ONLINE IP INFRINGEMENTS POST-GDPR	6
D.	RIGHTS ENFORCEMENT POST-GDPR	9
E.	WHAT ABOUT COUNTRY-CODE TOP-LEVEL DOMAINS?	12
F.	GOING FORWARD	13
G.	ACTION POINTS	14

A. WHOIS POST-GDPR

Background

The Registration Data Directory Service, also known as WHOIS, is a decentralised database containing information about registered domain names and their holders (registrants). This information includes, *inter alia*, the date of registration, the sponsoring registrar, and the name, postal address, telephone number and email address of the registrant.

Before the entry into force of the GDPR, interested parties could freely access this WHOIS information to, for example, identify the holders of fraudulent or infringing websites, to combat counterfeiting or to investigate cybercrime.

What has happened after 25 May?

After consultating the EU commission and national data protection authorities (DPAs), ICANN[1] decided it could no longer maintain an unrestricted publicly accessible WHOIS system for its generic top-level domains (gTLDs)[2] once the GDPR came into effect.

As a result, most of the WHOIS information, such as the registrants name, email address, postal address and telephone number are no longer publicly available, regardless of the registrant being a natural or legal person. WHOIS queries will now only display the registrant's organisation (if applicable), his country, state and/or province, and an anonymised email address or contact form, unless the registrant actively consents to the publication of additional information. Additionally, automated access and reverse WHOIS queries are no longer possible.

ICANN now aims to implement a 'layered access model' where interested entities such as law enforcement authorities, IP rightsholders, lawyers and cybersecurity organisations must first be accredited by a responsible body before receiving access to more or all WHOIS information.

However, the practical implementation of such a model could take years and is sure to meet opposition of contracted parties and privacy advocates. To avoid the fragmentation of WHOIS and maintain reasonable access to relevant WHOIS information for legitimate purposes, ICANN adopted a Temporary Specification containing obligations for registrars and registries concerning WHOIS.

The Temporary Specification and Reasonable Access to Non-Public WHOIS Data

The Temporary Specification for gTLD Registration Data aims to establish temporary requirements for registrars and registry operators to comply with the principles and obligations of the GDPR, while maintaining the availability of the

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

[2] Generic top-level domains are domain name extensions which are not attributed to a specific country (*cfr.* country-code top-level domains), such as .com, .biz, .org, .net, .law, etc.

WHOIS system and ensuring compliance with the existing contractual obligations vis à vis ICANN. It mandates, for example, the collection and transfer to ICANN and the registry operators of all "thick" WHOIS information.

However, until an accreditation and access model is effectively implemented, access to non-public WHOIS information can only be obtained from the sponsoring registrar or registry operator, who must provide "reasonable access" to such information on the basis of an overriding legitimate interest. Unfortunately for IP rightsholders, no mandatary set of consistent standards and processes to provide such "reasonable access" to non-public WHOIS information have been provided under the Temporary Specification. As a result, rightsholders are dependent on a discretionary decision by the applicable registrar or registry operator.

The lack of any further guidance by ICANN or the DPAs resulted in diverse responses from registrars and registry operators. Some provide expedient disclosure when presented with proof of IP right ownership and credible infringement. However, others demand a relevant court order before deciding on access. As a result, IP rightsholders are left in the dark to the case-by-case assessments made by the intermediaries.

What is next?

Since the Temporary specification can only be in place for one year, an expedited policy development process (ePDP) must flesh out the many outstanding issues, including the development of an effective and expedient accreditation and access model, and to establish a formal and consistent WHOIS and GDPR policy. However, certain stakeholders have already indicated that they want to exclude issues related to accreditation and access from the scope of the ePDP.

As we do not expect an effective access system to non-public WHOIS information in the near future, this guide aims to assist IP rightsholders to obtain the necessary information to enforce their rights in a post-GDPR landscape.

Contact Information

Registrant Contact
Name: REDACTED FOR PRIVACY
Organization: REDACTED FOR PRIVACY
Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY BE
Phone: REDACTED FOR PRIVACY
Ext:
Fax: REDACTED FOR PRIVACY
Fax Ext:
Email:Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Admin Contact
Name: REDACTED FOR PRIVACY
Organization: REDACTED FOR PRIVACY
Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY
Phone: REDACTED FOR PRIVACY
Ext:
Fax: REDACTED FOR PRIVACY
Fax Ext:
Email:Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Tech Contact
Name: REDACTED FOR PRIVACY
Organization: REDACTED FOR PRIVACY
Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY
Phone: REDACTED FOR PRIVACY
Ext:
Fax: REDACTED FOR PRIVACY
Fax Ext:
Email:Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

B. PLAYERS IN DOMAIN NAME REGISTRATION

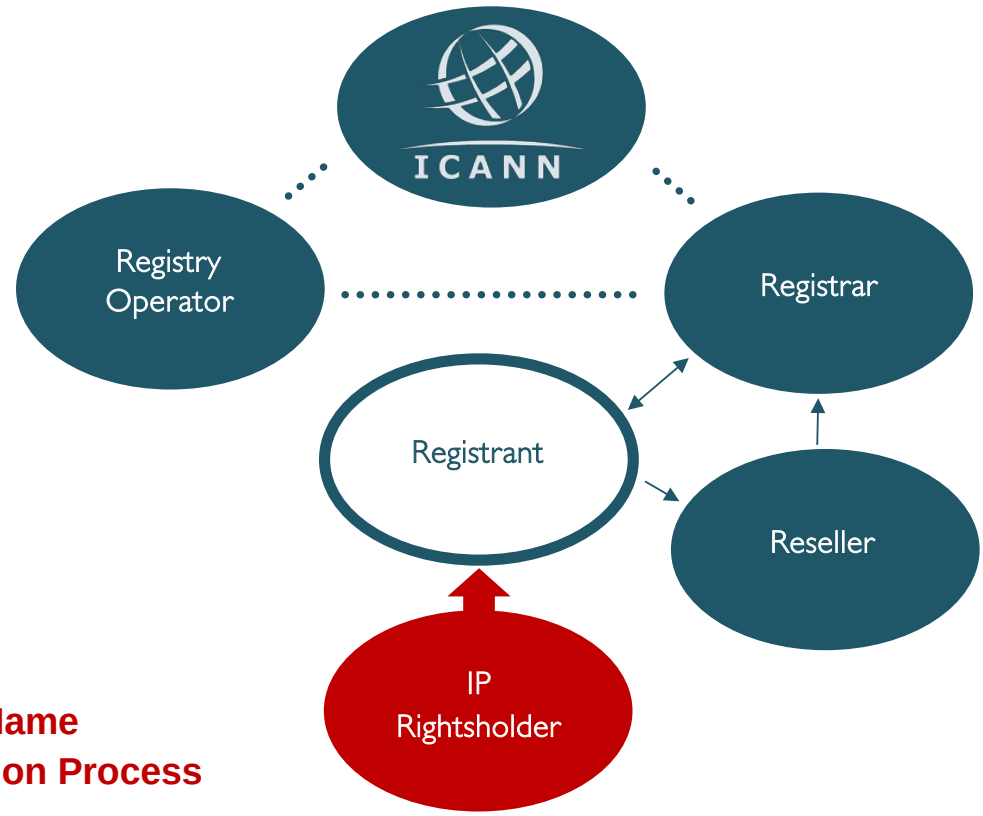
Distinguishing between Registrars

Domain name registrars are the primary recipients and holders of personal information of the registrant. Registrars are the main point of contact for IP rightsholders when they require non-public information on a potential online infringer.

Registrars must comply with ICANN's WHOIS policies and dispute resolution mechanisms as part of their contractual obligations under the Registrar Accreditation Agreement. They also enter into contracts with relevant registry operators to register domain names in their top-level domain.

There are currently approximately 2.500 accredited registrars, with some taking their contractual obligations more serious than others. Business-to-business registrars, focusing on domain name management and brand protection for their professional customers, generally have a reputation of strong compliance and provide expeditious access to interested third parties with a legitimate interest. IP rightsholders should engage with these registrars to obtain effective redress.

Other less specialised registrars have shown to prefer protecting the privacy of their customers, irregardless of legitimate access requests. This appears especially true for registrars providing privacy or proxy registration services. Any non-compliance should be directly reported to ICANN's compliance department.



Domain Name Registration Process

C. INVESTIGATING ONLINE IP INFRINGEMENTS POST-GDPR

Businesses and organisations can identify potentially infringing websites and domain names through a number of ways, such as automatic online scanning software, private investigations, customer complaints, rights protection mechanisms, etc.

When an infringing website and/or domain name has been identified and evidence of the potential IP infringement is collected, a rightsholder should secure the identity and contact information of the registrant to enforce its IP rights. Identifying the potential infringer is important for various reasons: to verify whether the operator of the website is a legitimate licensee or authorised reseller of the IP rightsholder; to determine whether the person holds other potentially infringing domains; or to start legal proceedings.

Without a freely accessible WHOIS system, rightsholders must apply other measures and strategies to obtain this important identity and contact information to effectively enforce their IP rights.

- Organisation of the registrant (if applicable)
- Country, state/province of the registrant
- Anonymised contact point (email address or web form)

← Public WHOIS

- Full name of the registrant
- Location / postal address of the registrant
- Telephone / fax number of the registrant
- Email address of the registrant
- Associated domain names / websites

← I. Disclosure request with registrar

← II. Substantive evidence

← III. Historic WHOIS data

← IV. Other public data sources

← V. Associated websites

← VI. Assistance by other intermediaries

I. Disclosure Request with the Relevant Registrar

A simple WHOIS search, performed for example on whois.icann.org, will continue to display the registrar of a specific domain name. Although we have already indicated that a standardised process to provide reasonable access is lacking, resulting in registrars reacting differently to disclosure requests, a disclosure request with the registrar may be the least onerous way to obtain the necessary information.
In order to be compliant with the GDPR, an access request should contain at least:

(i) the identity of the requesting party;

(ii) information on the relevant trademark or other IP right(s) owned by that party;

(iii) the potentially infringing domain name(s) and evidence on the credible infringement of the identified IP right(s);

(iv) the requested (personal) information necessary to investigate, prevent or combat the infringement; and

(v) a statement indicating that the request is based on article 6(1)(f) of the GDPR, providing that the identified legitimate interest of the requestor override the privacy interests of the registrant.

If a registrar refuses reasonable access to vital information, a rightsholder should not shy away from taking effective action by (i) contacting ICANN's compliance department indicating a violation of section 4.1. Appendix A of the Temporary Specification, or (ii) by taking legal action on the basis of general tort and by establishing contributory liability.

II. Website Content and Substantive Evidence

The website accessible via the domain name often contains important information which may (help to) identify the infringing party. Email addresses, logo's, tags, organisations, language and currencies displayed on the website may all contribute to form a picture of the registrant behind a particular domain name. The European E-Commerce Directive requires, for example, that online businesses provide clear identity and contact details on their websites. Evidently, complying with such regulations is often not the infringing registrant's first concern.

Additional information could also be established by using website crawlers and Internet archives which provide archived information or metadata connected to individual domains.

III. Historic WHOIS Data

Certain service providers have progressively collected existing WHOIS information to establish a repository which may reveal full identity and contact details on existing registrants of listed domain names before 25 May 2018. While this may prove extremely valuable for the moment, the relevance of these historic databases will evidently decrease over time. Additionally, questions can be raised as to their legitimacy in relation to the GDPR.

IV. Public WHOIS Data and Other Public Data Sources

Although limited, the WHOIS data that are currently publicly available may still provide essential information to identify the possible infringer. While unlikely, the registrant may have opted to consent to publishing additional information in the WHOIS system, such as

a name or email address. Additionally, the registrant's provided organisation, if applicable, may reveal a company or association behind an infringing individual, who could be identified by searching relevant commercial registers or trademark registries.

V. Associated Websites/ Domain Names and Social Media

Associated websites linked to the potentially infringing domain name can expose other infringements and/or reveal additional information about the registrant behind them. Rightsholders can track down these websites by following hyperlinks or redirections connected to the infringing domain name/website or by determining a hosting location using the websites' IP address. The fact that an IP address is black listed, may further indicate infringement.

More and more bad faith registrants are also using social media to attract Internet users to the websites connected to their infringing domain names. These social media pages can reveal a lot of personal information and/or other infringing domain names or content.

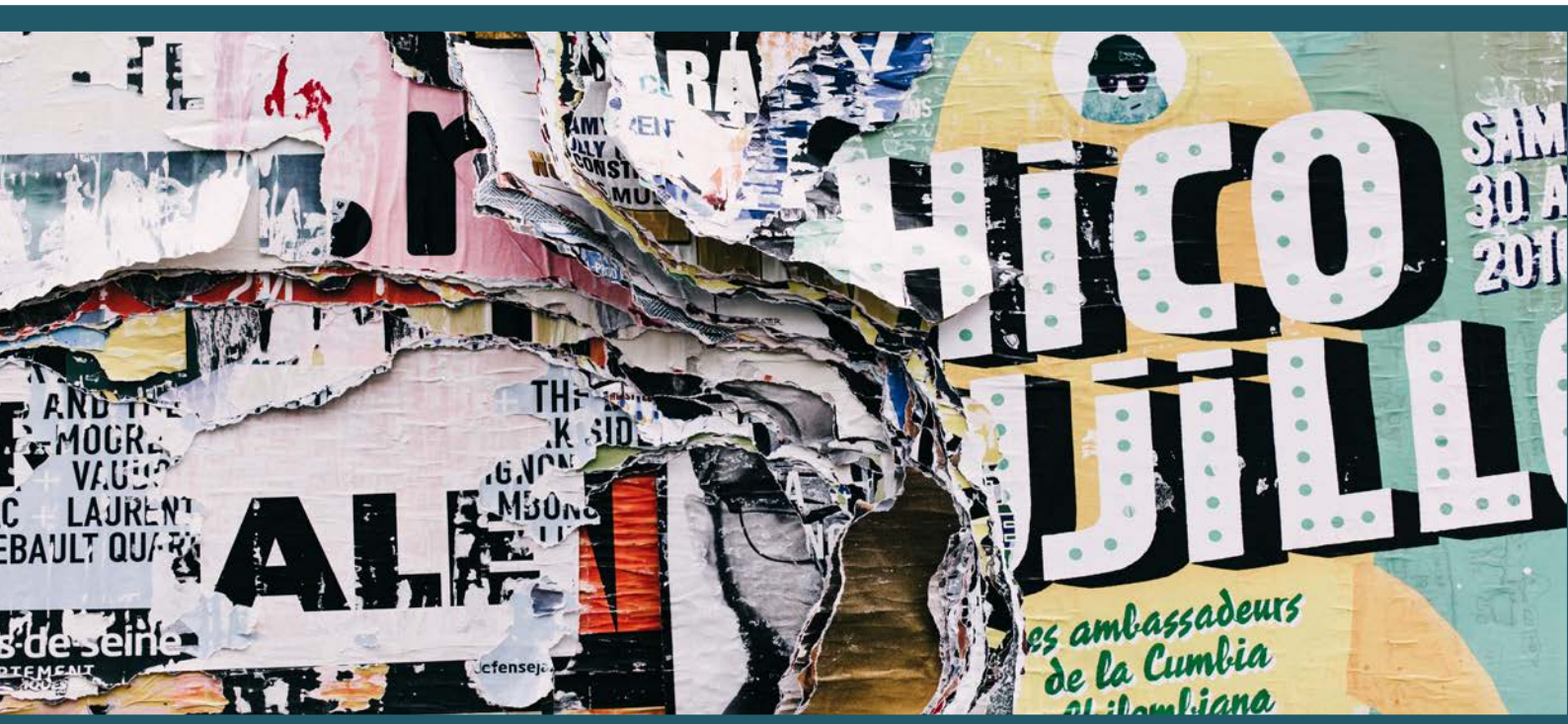
VI. Other Intermediaries

Next to the domain name's registrar, other intermediaries are in a position to disclose the identity or contact details of the registrant. Counterfeiting, illegal content or clear trademark abuse could all constitute a legitimate justification to request such data.

If counterfeited goods are sold on the website, a request can be filed with the payment service provider(s) used by the website. Additionally, the webhost or internet service provider (ISP) can be contacted to either relay communications to the domain name holder or provide further relevant information.

VII. Risk of registrant awareness

For all these measures to obtain information, IP rightsholders should always keep in mind that registrants may become aware of an investigation, leading them to further conceal their identity, cover up their infringing activity or dispose of the domain name altogether. The risk of "cyberflight" is particularly high when disclosure requests are relayed by an intermediary.



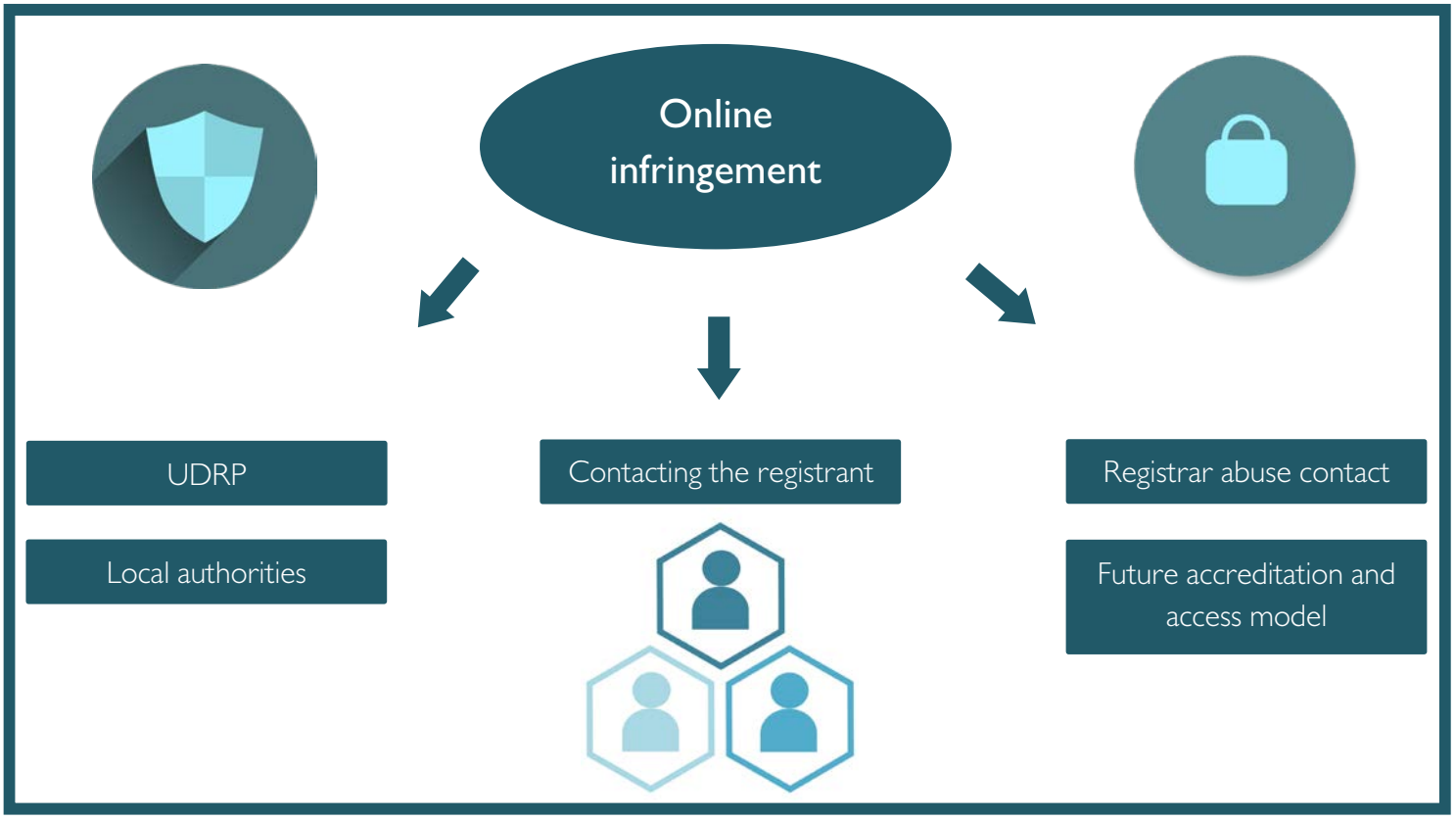
D. RIGHTS ENFORCEMENT POST-GDPR

Contacting the Registrant

Before starting administrative or court proceedings, IP rightsholders will often attempt to contact the alleged infringer first, to provide notice and demand the cease and desist of the infringement. An infringement may not always be apparent and communication with the holder of a domain may clear up any uncertainties or misconceptions, or lead to negotiations on the sale of a specific domain name.

While the registrant's contact information is no longer publicly accessible post 25 May 2018, ICANN's Temporary Specification does require registrars to provide for an anonymised email address or web form to be displayed in the public WHOIS records. Until an effective accreditation and access model is in place allowing accredited parties to access the contact details of the registrant, this email address or web form will be the only way to 'directly' contact the domain name holder. However, while registrars are required to forward any communication sent to these addresses, IP rightsholders often remain in the dark as to the conduct of the registrar and the delivery of the message to the registrant. Certain registrars, for example, first review the content of the communication before deciding to relay it to their customers.

Lastly, as mentioned above, an attempt to contact the domain name holder 'directly' may not always be the wisest choice, as it may prompt bad faith registrants to hide behind the obscurity of this relay mechanism and flee from any accountability.



Contacting the Registrar Abuse Contact

Registrars are required to maintain an abuse contact to receive reports of abuse involving their sponsored domain names. Abuse may cover anything from inappropriate content and violation of terms and conditions, to illegal activity and copyright or trademark infringements.

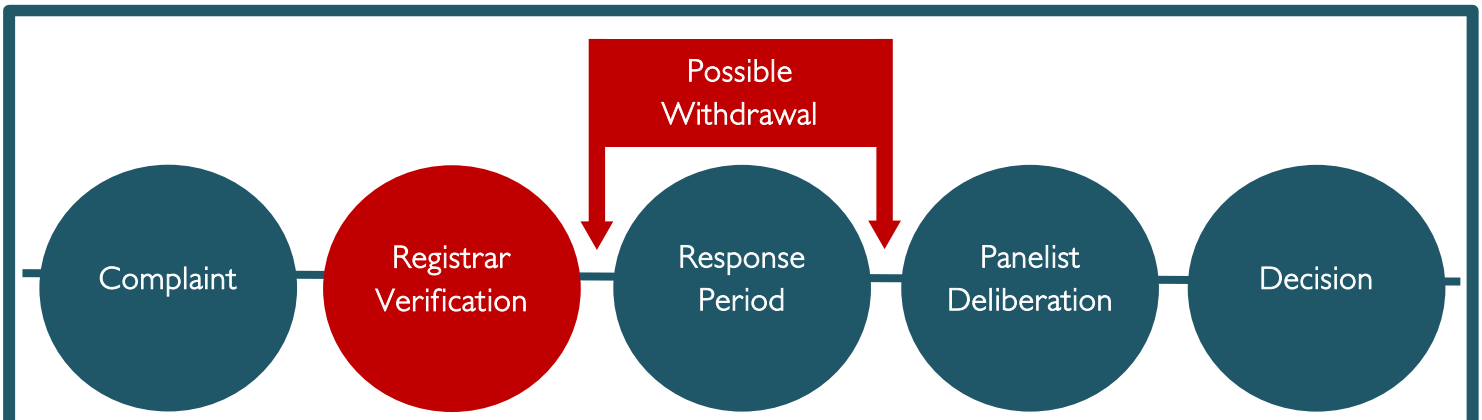
Registrars have a duty to promptly investigate abuse and take appropriate measures, which may include the disclosure of the registrant's identity and contact details, contacting competent law enforcement authorities, or cancelling the infringing domain name. Failure to do so constitutes a direct violation of the registrars' accreditation agreement for which a rightsholder may file a complaint with ICANN's compliance department.

Initiating UDRP Proceedings

Trademark owners facing bad faith registrations of domain names identical or similar to their trademarks, have a strong administrative measure available in the form of the Uniform Domain-Name Dispute-Resolution Policy (UDRP) or its accelerated (albeit less successful) alternative, the Uniform Rapid Suspension System (URS).

A UDRP Complaint must contain all the registrant information available. When the registrant's name and contact information is not available, a "doe" complaint may be filed against an individual "Redacted for Privacy". This is similar to previous UDRP Complainants filed against a WHOIS privacy or proxy service. After a complaint has been received by a dispute resolution service provider, the sponsoring registrar has the obligation to disclose the identity and contact details of the registrant and apply a "lock" on the domain. One of the clear advantages of initiating UDRP proceedings is that such a lock prevents "cyberflight" of the registrant.

Once the dispute resolution provider has received the personal information of the registrant, it will be relay that information to the complainant, who then has the option to either maintain its complaint with the redacted information, amend it to account for the new relevant information, or withdraw the complaint. Withdrawal may be warranted if the information proves that,



UDRP Proceedings Timeline

for example, the registrant had a legitimate interest as an approved reseller, he/she did not act in bad faith, or the matter is better settled between parties.

WIPO has indicated that upon such withdrawal, the unused panel fee will be refunded (*i.e.* USD 1,000 for a single-panel UDRP case involving 1-5 domain names). As a result, only the administrative filing fee must be paid to obtain the identity and contact details of the registrant (*i.e.* USD 500 for the above-mentioned matter). The Czech Arbitration Court (CAC) has also indicated to refund half of the administrative fees (*i.e.* EUR 400) upon such withdrawal.

However, the preparation of an unnecessary UDRP complaint can take up valuable efforts and costs which could be avoided if other, more appropriate investigatory or enforcement measures were considered. As a result, rightsholders must first make a careful case-by-case assessment on the available evidence and information and the potential risks, before opting to use one or several of the measures available to them.

Addressing Local Authorities

In cases where online infringers engage in an activity violating consumer or criminal law, such as counterfeiting, fraud or piracy, rightsholders and customers can also address local authorities, such as economic inspection units, customs or law enforcement. Jurisdiction of the competent authorities can be established on the basis of information still displayed in public WHOIS records, such as the registrant's country, state and/or province.

Evidently, court proceedings can also be initiated against online IP infringements. However, as many jurisdictions don't recognise *in rem* actions against domain names, unlike for example the U.S. or Germany, the identity of the infringing party remains a prerequisite to initiate these proceedings.

Future Accreditation and Access Model

IP rightsholders should engage with ICANN and relevant interest groups to achieve an effective accreditation and access model as soon as possible. The model must allow accredited parties to expeditiously obtain all necessary information to investigate IP infringements and enforce their rights without alerting the infringer. Such access must also support good-faith filings of UDRP complaints by allowing sufficient access to registration data necessary to evaluate and supplement prospective complaints.

E. WHAT ABOUT COUNTRY-CODE TOP-LEVEL DOMAINS?

Different WHOIS Policies

Country-code top-level domains (ccTLDs), such as .us, .uk, .fr, .be, and .eu, do not fall under ICANN's WHOIS policy. Each national registry operator must adopt a GDPR-compliant WHOIS model. The currently approximately 240 registries registries have adopted different models, some allowing easier access for the public and interested third parties than others.

EURid and .EU

For the moment, EURid, the registry operator of the .eu ccTLD, continues to display the registrant's language and email address in their public WHOIS records. EURid also makes a clear distinction between natural persons and legal entities, displaying more information on the latter.

However, a new EU legislative initiative has been launched which proposes to remove all information from public WHOIS unless the registrant has actively consented to publishing more information. As this completely negates the public interest aspect of WHOIS data, IP interest groups are already pushing back on this language.

Other Registry Operators

Other registry operators, such as Nominet UK for .uk or DNS Belgium for .be, have generally chosen to redact public WHOIS information of private persons altogether. Interested parties can still file individual access requests to obtain necessary information. These requests will be evaluated by the registry operator to assess whether the provided legitimate interest overrides the privacy interest of the registrant.

SIDN for .nl and ISNIC for .is, maintain that the publication of the registrant's email address remains necessary. SIDN does, however, provide for an opt-out system for registrants.

Charging for Access to WHOIS

Some registry operators, such as Nominet UK, have also indicated to charge interested parties for individual access requests. While this could be acceptable for ccTLDs with limited access requests, such a model must be avoided for a general access model which requires frequent persistent access.

F. GOING FORWARD

Towards an Accreditation and Access Model

Protecting IP online will never be the same post 25 May 2018. While the Temporary Specification is (as its name leads to expect) only temporary, it may permanently close the door on the WHOIS system as we knew it.

Until an effective accreditation and access model is implemented, IP rightsholders and other interested third parties will be dependent on more limited measures to obtain information, such as the discretionary decision of an intermediary.

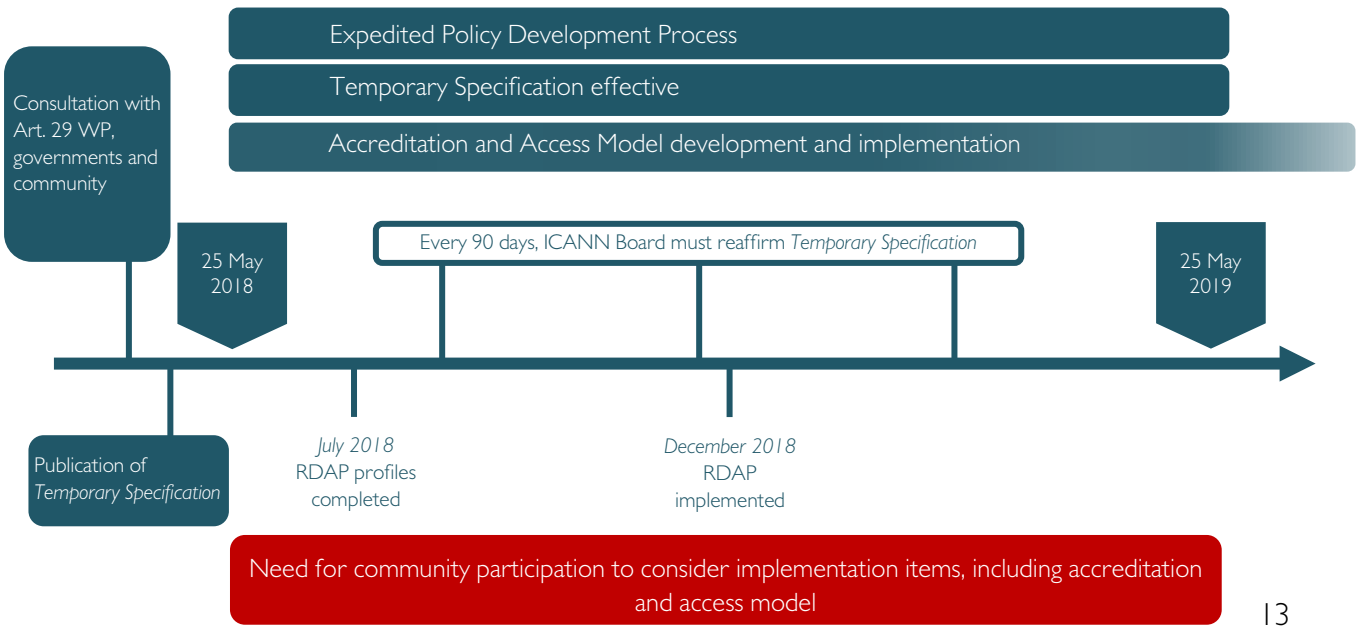
It is vital that the adoption of the accreditation and access model is included within the remit of the ePDP and that important issues as to its effectiveness are considered. For example, accredited parties showing a legitimate interest should receive access to all necessary information to pursue effective action without the need to rely on other alternative measures for additional data. Registrants should not be alerted of an access request to avoid cyberflight or cover-up.

Towards a Central ICANN-Administered Model?

The implementation of a layered accreditation and access model implies that the classic WHOIS system is adapted into the new Registration Data Access Protocol (RDAP). It would allow for a change in the current WHOIS organisation, where registration data are currently collected, organised and disclosed in a decentralised way by registrars and registry operators.

Voices have been raised to implement a central RDAP model, where ICANN - instead of individual registrars - would act as the primary administrator of the registration data system and provide reasonable access to necessary information.

Temporary Specification Implementation Timeline



G. ACTION POINTS

Rightsholders should take a strong collective position for WHOIS Access:

- Do not agree with a WHOIS system based on the sole discretion of registrars and registry operators. Essential information must be accessible to other entities with a legitimate interest.
- Contest that registrants should be asked for their consent to provide vital identification and contact information. WHOIS serves a public interest and must ensure the accountability of domain name holders.
- Advocate for balance with other important legal frameworks, such as regarding law enforcement, access to and free flow of information, consumer protection and the protection of intellectual property.

Rightsholder should consider various actions to safeguard effective IP protection and enforcement online and ensure that their interests are taken into account:

- Document and report any difficulties to obtain important WHOIS information, such as registrars refusing reasonable disclosure or failing to act on abuse complaints. Issues can be reported to WHOISchallenges@inta.org and info@petillion.law.
- Support reputable registrars who comply with their obligations towards ICANN and their customers, and endorse the implementation of a balanced WHOIS system.
- Engage with ICANN, EU authorities and/or national DPAs to push for a fast implementation of a balanced and effective accreditation and access model, or at least an accelerated interim solution to provide 'reasonable access' to vital information.
- Maintain enforcement efforts and consider taking action against non-compliant intermediaries through ICANN's compliance department or on the basis of (contributory) liability to infringement.

Contact information

We are members of the Brussels Bar

Offices

GG 126
Guido Gezellestraat 126
1654 Huizingen
Belgium (Europe)

Contact

info@petillion.law
T. +32 2 306 18 60
F. +32 2 306 18 69

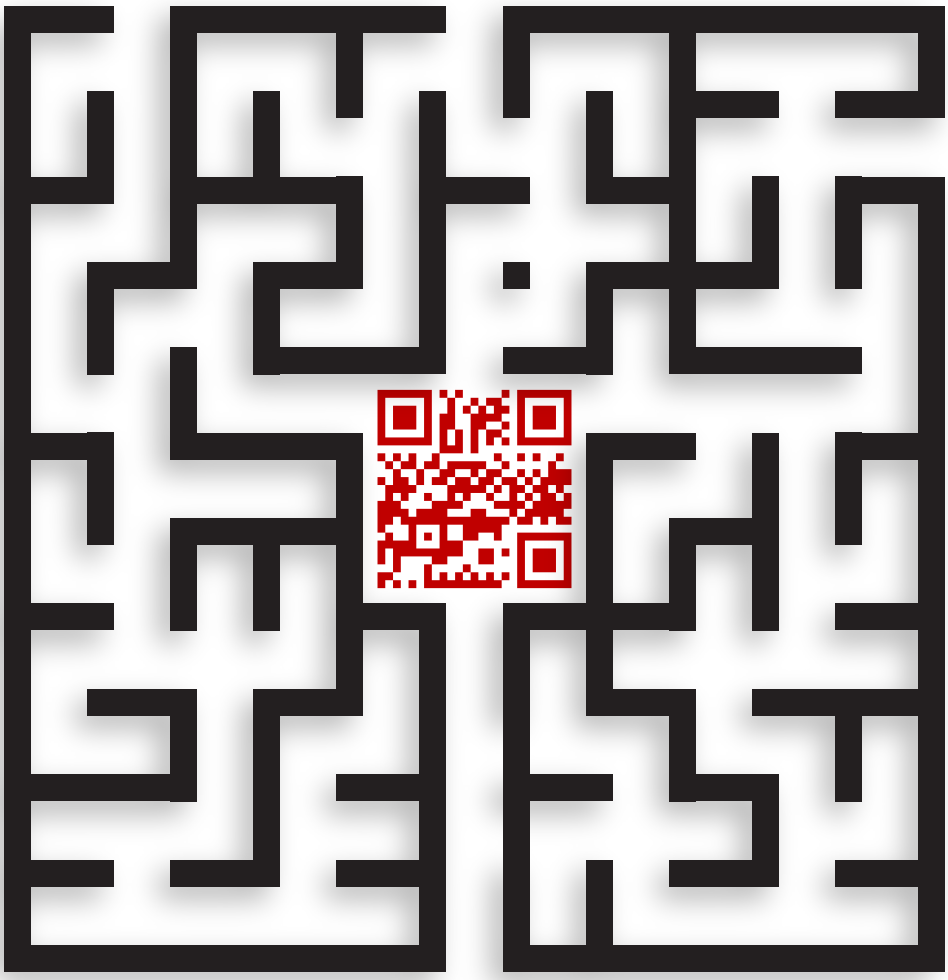
www.petillion.law

Time zone

West Coast	East Coast	London	Petillion	Abu Dhabi	Singapore	Sydney
UTC -8	UTC -5	UTC	UTC +1	UTC +4	UTC +8	UTC +11
PST	EST		CET	GST	SGT	AET

Petillion

Attorneys - Advocaten - Avocats



Your gateway to dispute resolution

www.petillion.law