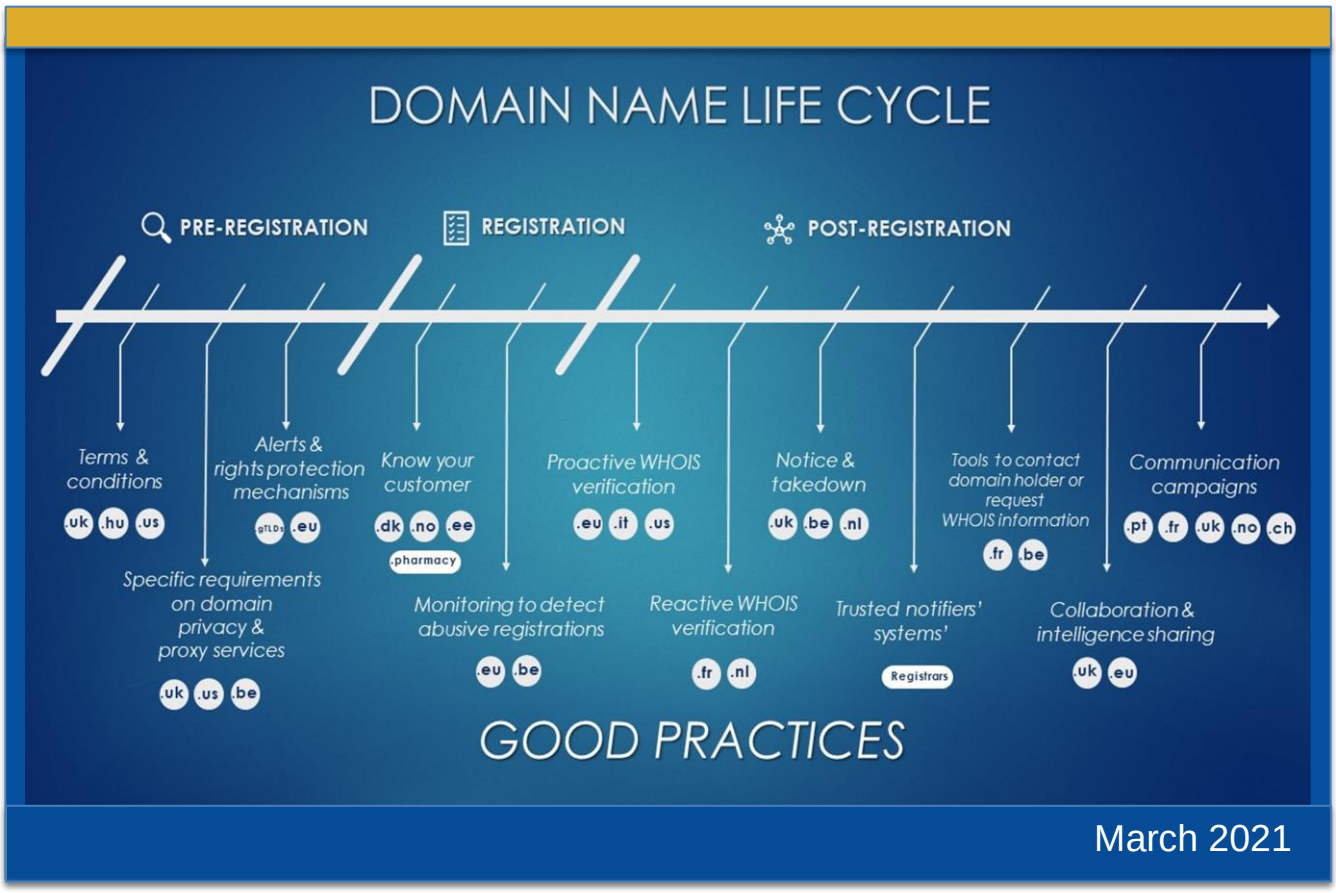
EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

DOMAIN NAMES – DISCUSSION PAPER

Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities



March 2021

DISCLAIMER

The views expressed in this discussion paper do not represent the official position of the EUIPO. This paper is based on the work of the EUIPO Observatory's Expert Group on cooperation with intermediaries. The views expressed in this discussion paper cannot be attributed to the Expert Group as a whole or to any single contributing expert.

The Observatory welcomes any further input or comments on this discussion paper, to continue deepening its understanding of good practices in undermining the misuse of domain names for IP-infringing activities. This discussion paper may be subject to reviews or updates, based on any further input from experts or new developments in the field.

ISBN 978-92-9156-287-9 doi: 10.2814/238062 TB-02-21-137-EN-N

Table of Contents

1. Foreword

The Expert Group on 'Cooperation with intermediaries' was set up to further the understanding of different intermediary services, how they can be misused for IP-infringing activities, and what the good practices are to undermine such misuses. This first discussion paper looks into Domain Names. It will hopefully contribute to a better understanding of the domain name ecosystem, the good practices that are developing to prevent the misuse of domain names for IP-infringing activities, and the challenges and opportunities to extend or replicate some of these good practices.

2. Executive Summary

This discussion paper provides an overview of the good practices that can help prevent the misuse of domain names for IP-infringing activities. This is the case when IP rights are misused in the name of the domain itself (i.e. cybersquatting or typosquatting) or when the domain name leads to a website supporting IP-infringing activities.

While the rules governing generic top-level domains (gTLDs) and country code top-level domains (ccTLDs) are different, the lifecycle of a domain name is the same for all TLDs. It can be divided into three main phases: pre-registration, registration and post-registration. A number of good practices from different registrars and registries have been identified in each of these phases.

Pre-registration: A number of registries have terms and conditions that clearly list IP rights (IPRs) infringement as one of the breaches of contract that can lead to suspension of a domain. Some registries also prohibit or limit the use of proxy services which in many instances are used by bad faith actors. In addition, some alerts and rights protection mechanisms have been developed for trade mark owners to be informed when a domain name identical to their trade mark is registered, so that they can take appropriate action.

Registration: Some registries have put in place systems to verify the identity of the registrant, using electronic identification solutions, and/or public registries. In addition, some registries have developed systems to automatically detect abusive domain registration applications and suspend them.

Post-registration: Some registries do manual or automated checks to detect fake or incorrect registration information, after the domain name has been registered. Some do the checks proactively, while others have put in place verification request processes. Some registries have also put in place notice and takedown (NTD) processes, to be used for notifying domains with illegal content. Such NTD schemes are typically developed in cooperation with public or law enforcement authorities, to limit the liability of the registry in case of a wrongful takedown. A number of registrars have also developed cooperation agreements to put in place 'trusted notifiers' systems.

In addition to the above, some registries are cooperating with IP owners and enforcement authorities to share intelligence and limit IP-infringing uses of domain names. Several registries also conduct awareness-raising activities to teach their national communities about illegal activities taking place through the use of domain names.

The good practices identified are typically implemented by a limited number of registrars and registries. In that respect, the discussion paper lays out the challenges and opportunities to extend each practice, taking into consideration that registrars and registries of all sizes have different economic and technical resources.

3. Introduction and Background

The Domain Name System (DNS) is indispensable to the functioning of the internet, as it turns machine-readable internet addresses into website names that people can understand. The number of domain names keeps growing. According to the CENTR ([1]), as of April 2019, '[t]he global TLD [top-level domain] market [was] estimated at around 351 million domains across 1 486 recorded TLDs. […] [N]ew gTLDs, which include well over 1 000 TLDs, have a little under 10 % of the market …' ([2]). As of April 2020, the global market had grown to an estimated '375 million domains under management with a split of 66 % to gTLDs and 34 % to ccTLDs' ([3]).

3.1 Categories of IP-infringing business models

Domain names also play a central role in a number of IP-infringing online business models that were identified in research by the 2016 EUIPO Observatory on infringements of IP rights (the Observatory) ([4]). These business models can be divided into two main categories.

- **Business models where IP is misused in the domain name**: '[c]ybersquatting means registration and use of a domain name that is identical or confusingly similar to another's trade mark and where the registration and use is in bad faith and with the intention to somehow profit from the registration and use. A variation of cybersquatting is *typosquatting* where a registrant acquires misspellings of other's domain names with the intention of catching and exploiting the traffic that was intended for the genuine websites. Both phenomena continue to take place in high numbers, which may be explained not only by the implementation of the many new generic top-level domains such as .xyz and .top, but also by the continuous development of ways to gain revenue from such registrations such as 'pay-per-click' revenues and revenues based on affiliate advertising schemes ([5]).'

- **Business models where the domain name leads to a website supporting IP-infringing activities**: many IP-infringing business models, including websites marketing and/or providing links to counterfeit goods or pirated content, are 'operated through an Internet site that is controlled by the infringer which means that the infringing entity (or its proxy) is the registrant

([1]) Council of European National Top-Level Domain Registries.
([2]) CENTR, CENTRstats Global TLD report 2019/1, Q1 2019 – Edition 27.
([3]) CENTR, CENTRstats Global TLD report 2020/2, Q2 2020 – Edition 31.
([4]) EUIPO, Research on Online Business Models Infringing Intellectual Property Rights Phase 1, July 2016.
([5]) EUIPO, Study on legislative measures related to online IPR infringements, September 2018, p. 21.

of the domain name and the content of the website is made available by the infringer' ([6]). Such IP-infringing websites often re-register previously used domain names, 'to benefit from the popularity of the website that was previously identified by the domain name' ([7]). Other practices include registering multiple domains for the same site to circumvent enforcement measures directed at one domain ([8]), or even the registration of the name of a popular IP-infringing site with a different domain by a new 'operator'.

It is important to note that these two business models can coexist, for example the registration of a domain name using a registered trade mark to sell counterfeit products under this trade mark.

The Observatory has led several studies to analyse the regulatory measures and dispute resolution mechanisms that address the use of domain names to infringe IP, notably:

- the *Study on legislative measures related to online IPR infringements*, which looked into a number of regulatory measures available in EU Member States to suspend, transfer, cancel or seize domain names ([9]);

- the *Comparative case study on alternative dispute resolution systems for domain names disputes* ([10]), which looked into dispute resolution policies for 10 different domains, and the likely outcome of disputes, including for websites infringing IP.

3.2 Challenges in addressing IP-infringing uses of domain names

A number of the EUIPO Observatory's stakeholders regularly highlight the issues raised by IP-infringing uses of domain names, in particular following on the extension to new generic TLDs in 2011.

They also point to the new restrictions on accessing WHOIS information on domain name holders following on the General Data Protection Regulation (GDPR) that came into effect in May 2018 ([11]).

([6]) Ibid. footnote 4, p. 9.
([7]) Research on Online Business Models Infringing Intellectual Property Rights – Phase 2, October 2017, p. 11.
([8]) e.g. movie4k.to, movie4k.pe.
([9]) Ibid, footnote 5, pp. 47-51.
([10]) Comparative case study on alternative dispute resolution system for domain names disputes, February 2019.
([11]) 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 (General Data Protection Regulation).

In March 2020, the Governmental Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN)([12]) stated that '[r]easonable access to [WHOIS] information is essential to allow public authorities and other relevant entities to serve objectives such as law enforcement, cybersecurity, consumer protection or the protection of intellectual property'([13]).

Since IP infringers rarely use their real contact details, these restrictions have a limited impact on the capacity of IP owners to effectively identify the holder of a domain name used for IP-infringing activities. However, they do hinder IP owners' ability to identify contact details that are obviously fake and ask for a verification of the domain name holder's identity and reduce the capacity of law enforcement authorities to identify fraudulent activities or patterns. Experts consider these identity verifications to be a very effective way of dealing with domains supporting IP-infringing activities (see section 4.3).

Experts point to a number of other challenges in dealing with IP-infringing uses of domain names, in particular the following.

- The use of **domain privacy([14]) and proxy([15]) services** that act as intermediaries for domain registrations, with the contact details of the proxy service appearing in the WHOIS data instead of the contact details of the actual registrant([16]). These services are often located in jurisdictions where it is difficult to request and obtain information on their users. A study commissioned by ICANN in 2013 established that '[a] significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity'([17]).

([12]) The Governmental Advisory Committee (GAC) 'serves as the voice of Governments and International Governmental Organizations in ICANN's multi-stakeholders representative structure'. It has 178 members. See the ICANN / GAC webpage.
([13]) GAC Communiqué – ICANN67 Virtual Community Forum, March 2020, p. 7
([14]) From ICANN's website: 'Privacy services allow a domain name holder (registrant) to be listed as the registrant of record but with alternate, valid contact information (such as a mail-forwarding service address) published in place of the registrant's home address.'
([15]) From ICANN's website: 'Proxy services allow a domain name to keep certain identity and contact details from appearing in public Whois information. The proxy service becomes the registered name holder of record, and its identity and contact information is displayed in Whois data.'
([16]) Domain privacy and proxy services are originally meant for registrants who do not wish their private data to be displayed on web-based public WHOIS services. They are typically used in jurisdictions lacking proper data protection regulation such as GDPR.
([17]) A study of Whois Privacy and Proxy Service Abuse, September 2013.

- The **use of stolen individual or business details** to register a domain used for IP-infringing activities ([18]). This undermines the measures put in place to detect abusive domain name registration by looking into inconsistent registration data (see section 4.2.2), as well as any action against the individual or business listed as the domain name registrant, who may be the unknowing victim of an identity theft.

- The use of **subdomains to 'hide' infringing content**, which is an emerging trend for websites selling counterfeits. If the domain itself (e.g. domain.com) does not have any content and appears to be offline, counterfeits are sold through pages appearing on a subdomain (e.g. subdomain.domain.com). These subdomains are promoted and communicated directly to users through multiple channels, including social media. This makes it more difficult to check and establish if a specific domain is used for IP-infringing activities.

- The use of **dispute resolution mechanisms** to address infringing use of a trade mark in a domain name, as some experts question whether the Uniform Domain-Name Dispute-Resolution Policy (UDRP) in its current format is a viable or cost-effective option, given the sheer volume of domains that are registered and that are infringing IP.

4. Scope and Approach

In this context, the Observatory has initiated work to identify good practices by registrars and registries in preventing the use of domain names for IP-infringing activities and explore if some of them could be replicated by EU country code TLD (ccTLD) registrars and registries.

The Observatory asked its Expert Group on cooperation with intermediaries ([19]) (the Expert Group) to support its work in that field. This discussion paper reflects the work and discussions with the Expert Group. It describes the life cycle of a domain name and the respective roles of registrars and registries throughout this cycle. It establishes a list of good practices, distinguishing between registrars and registries. It covers all existing or developing good practices at a global level, and is not limited to good practices by EU ccTLD registrars

([18]) For examples of such practices, see Identity theft by domain name; what Afnic does, September 2018.

([19]) The EUIPO Observatory Expert Groups help and guide the implementation of Observatory projects in focused and specialised areas, in this case 'cooperation with intermediaries'. Experts are called upon to provide expert support to the Observatory's agreed projects and activities. Experts represent themselves and not a particular organisation or institution.

and registries. It also covers technical measures put in place by some registries to prevent or terminate IP-infringing uses of domain names.

Considering the number of registrars and registries at the global level, this discussion paper does not aim to catalogue all good practices by all players, but rather to establish broad categories of good practices based on concrete examples. Good practices are listed according to the different stages of a domain name life cycle, distinguishing between proactive and reactive measures.

When identifying challenges or opportunities to extend the good practices identified, this discussion paper focuses on European ccTLD registrars and registries. It looks into the specific regulatory, economic and technical challenges faced when replicating each of the good practices identified, taking into consideration the fact that there are registrars and registries of all sizes, with different economic and technical resources.

5. The Domain Name Life Cycle and the Respective Roles of Registries and Registrars

5.1 Registries and registrars

Registries and registrars have different but complementary roles in the life cycle of domain names. It is important to clearly distinguish the two and to clarify their respective roles and obligations.

According to ICANN glossary, a domain name **registry** can be defined as the authoritative, master database of all domain names registered in each top-level domain ([20]). A similar definition, focusing on **registry operators**, is provided in Article 2 of Regulation (EU) 2019/517 on the implementation and functioning of the .eu TLD (Regulation 2019/517), according to which 'the Registry' means the entity entrusted with the organisation, administration and management of the .eu TLD, including the maintenance of the corresponding databases and the associated public query services, the registration of domain names, the operation of the Registry of domain names, the operation of the Registry's TLD name servers and the distribution of TLD zone files across name servers ([21]).

([20]) https://www.icann.org/resources/en/glossary#r (information retrieved on January 2020).
([21]) Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004.

Typically, the registry operator has more of a technical role, maintaining the master database of all domain names registered in a specific TLD and generating the zone files, which allow computers to route internet traffic to and from these domains ([22]). ICANN, through its supporting organisations and other constituencies, plays a central role in defining technical standards to preserve the stability of the Domain Name System ([23]), and both generic TLD (gTLD) and ccTLD registries have to comply with its policies concerning technical interoperability and TLD performance. However, the legal basis for the delegation and operation of registries differs for gTLDs and ccTLDs.

- **Generic top-level domains (gTLD)**: ICANN sets contractual obligations and enters into registry agreements with the different registries. As part of these obligations, gTLD registries have to comply with ICANN's 'Consensus Policies and Temporary Policies' ([24]). This includes the UDRP, which sets the policy on resolving trade mark-based domain disputes that may arise from abusive domain registrations. ICANN Registry agreements also require every accredited registry to periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, or botnets, and maintain statistical reports of the security threats identified ([25]).

- **Country code top-level domains (ccTLD)**: the process of delegation to a ccTLD registry and the obligations applying to such a registry are in many cases governed by national rules, or by EU regulations in the case of the .eu TLD ([26]). As a result, the ccTLD policies regarding registration and accreditation of registrars and WHOIS are independent and may differ from the policies set by ICANN ([27]). In many instances they reflect national public policy objectives, and in particular the need to ensure high standards of safety and security for the users of a specific ccTLD. This leads to a situation where a number of ccTLD registries have stricter rules on registration and on verification of the identity of the registrants, for example (see section 4.2).

In general, domain name registrants do not interact directly with the registry operator, but rather register domain names directly through registrars ([28]). **Registrars** are entities providing domain

([22]) https://www.icann.org/resources/pages/zfa-2013-06-28-en.
([23]) https://www.icann.org/resources/pages/cctld-2012-02-25-en.
([24]) https://www.icann.org/resources/pages/registrars/consensus-policies-en.
([25]) ICANN Registry Agreement, Specification 11(3)(b).
([26])There are many models of ccTLD governance globally, from regulated to fully self-regulated.
([27]) https://www.icann.org/resources/pages/cctld-2012-02-25-en.
([28]) https://www.icann.org/resources/en/glossary#r (information retrieved on January 2020).

name registration services to the public on the basis of an accreditation agreement with the relevant registry ([29]). An accredited registrar, acting on behalf of its users, can request registration, modification or deletion of information in the registry database. In some cases, a registrar might be the same entity that operates a registry, although these roles are typically split to allow for competition between multiple registrars offering different levels of price and support to domain name registrants ([30]).

If a registrant chooses to register a domain name under a specific TLD, they will be subject to the Terms of Use or Registration Policy of the registry operator, while the management of their domain will be performed by their designated registrar.

Accreditation agreements impose a number of technical, operational and financial obligations on registrars. While the obligations are broadly the same for gTLD or ccTLD registrars, here again the accrediting entities and the legal basis for the obligations imposed on registrars differ.

- **Generic top-level domains**: to enter into an accreditation agreement with a gTLD registry, the registrar first has to be accredited by ICANN. The accreditation obligations for the base gTLD registrar agreement are set and governed by ICANN ([31]). With regard to the .com gTLD, for example, registrars are required under ICANN based contractual obligations ([32]) to provide customer-related services, adhere to the registry's consensus policies ([33]), populate WHOIS data in a timely manner and provide public access to it, require domain name holders to enter into a registration agreement and investigate contact information reported as inaccurate ([34]). Once accredited by ICANN, the registrar can indicate the gTLDs for which they want to offer registration services, but they will still need to conclude accreditation agreements with the specific registry operators whose gTLDs they wish to service.

- **Country code top-level domains**: registrars are accredited by national registries on the basis of contractual obligations based on local rules, or on Regulation 2019/517 for the .eu TLD.

([29]) Article 2 of Regulation 2019/517 defines a registrar as 'a natural or legal person that, on the basis of a contract with the Registry, provides domain name registration services to registrants'.
([30]) https://www.icann.org/resources/en/glossary#r (information retrieved on January 2020).
([31]) https://www.icann.org/resources/pages/accreditation-2012-02-25-en.
([32]) https://www.icann.org/resources/pages/what-2013-05-03-en.
([33]) ICANN, Consensus Policies.
([34]) https://www.icann.org/resources/pages/what-2013-05-03-en.

The compliance of accredited registrars with their contractual obligations can be assessed by ICANN ([35]) or relevant registries, and may lead to the suspension or termination of the agreement in the case of repeated breaches ([36]).

5.2 Domain name life cycle

For the purposes of this discussion paper, the typical domain name life cycle is divided into three phases, namely pre-registration, registration and post-registration.

5.2.1 The pre-registration phase

Availability check: the registry usually provides internet users with the ability to check the availability of the domain name they want to register ([37]). At this stage, domain names already registered can be challenged if the registration is deemed to abusively prevent a user from registering a domain name of their choice (see section 3.2.3).

Application to the registrar: a user wishing to register a domain name will have to designate a registrar that is accredited for the TLD of their choice and submit an application to register the desired domain name. As part of the application process the user is usually required to provide:

- information and contact details of the registrant (including email address, physical address and contact phone number);
- administrative and billing contacts;
- the desired registration terms;
- payment information.

Based on the registrant's request, the registrar checks the registry database to ascertain the availability of the desired domain name and initiate a 'create domain' transaction. If the registration is successful, it creates a WHOIS record based on the registrant's information. Part of the registration process is the registrant's acceptance of the terms and conditions of use (see section 4.1.1).

([35]) ICANN, Registrar Compliance Program 2016.
([36]) ICANN, Three Registrars Lose ICANN Accreditation; EURid, Notice Of Termination Of Registrar Accreditation Agreements, February 2015.
([37]) https://eurid.eu/en/; https://www.nominet.uk/whois/.

5.2.2 The registration phase

Registration with a registry: upon registration, the registry can either immediately activate the domain name, or perform a set of checks and/or risk assessments before doing so (see section 4.2).

Duration: sometimes, registrants can decide on the duration of the domain name registration (especially for gTLDs), which is usually from 1 to 10 years and can be renewed, subject to the payment of renewal fees. In other cases (especially that of ccTLDs), the registration is for a specific duration (usually 1 year) and can be renewed, subject to the payment of renewal fees. For some TLDs the period of registration is indefinite, provided that there are no reasons for the domain name to be terminated ([38]).

5.2.3 The post-registration phase

Delegation: this is a technical operation consisting in linking a registered domain name with the location where the content related to this domain name (e.g. a website) is hosted. With the delegation, a DNS server receiving a request to access a domain name can resolve this request and retrieve the correct location where the relevant content is hosted. Without the delegation, the DNS server cannot retrieve the correct location, and will typically return an error message. In practice, this means that before delegation, a website with a registered domain name cannot be accessed.

Renewal: registrants are responsible for renewing their registration, including paying renewal fees. As part of the services provided to registrants, registrars usually send reminders before the expiration of a domain name and perform all the tasks related to the renewal, including the payment of the renewal fees ([39]).

Expiration: a registration expires and the domain name is deleted from the registry database if it is not renewed, or if the registrant asks the registrar to cancel the registration ([40]). In both cases, registrars are required to delete the domain names from the registry database. Registries usually provide for auto-renewal and redemption grace periods. During these periods, the domain name deletion is pending, and it cannot be registered by another registrant.

Check on WHOIS data: automated and/or manual verification of WHOIS data is performed by a number of registries to identify fraudulent domain name registrations. ‘A registry’s Terms and

([38]) Article 15 of SIDN General Terms and Conditions of service for registrants.
([39]) Article 6, EURid Accreditation Agreement V.6.0.
([40]) https://www.icann.org/resources/pages/domain-name-renewal-expiration-faqs-2018-12-07-en.

Conditions usually explicitly require the domain name holder to provide correct data and contact details upon registration and keep this information up to date. Providing false or incorrect data is a violation of the Terms and Conditions and can lead to the deletion of a domain name ([41]).' Such checks, with the registry asking a registrant to confirm their data and contact details, can be performed:

- on the registry's own initiative (see section 4.2);
- in response to a report or complaint about false registration data (see section 4.3.1).

Disputed domain name: if a natural or legal person wants to challenge a domain name registration, most registries have put in place alternative dispute resolution (ADR) services ([42]), or will refer complainants to an external ADR service ([43]). If no internal or external ADR services are available, the registry will resort to standard legal procedures such as court litigation.

Notice and takedown: some registries have put in place notice and takedown procedures and collaboration with law enforcement authorities to deal with websites posting unlawful content (see section 4.3.2).

Domain name status: a domain name can have a different status depending on a number of actions taken at the time of its registration or afterwards.

- **Locked**: the deletion, update or transfer of a domain name can be prohibited to prevent unauthorised changes that may result from fraud ([44]). The prohibition of such changes can only be lifted by contacting the registry.

- **Suspended**: this can be the case when a registrant does not answer a request to confirm their data ([45]), or when a domain name is used for unlawful activities ([46]).

([41]) CENTR policy document on 'Domain names registries and online content', p. 18.
([42]) This is notably true in the case of Nominet: https://www.nominet.uk/domain-support/uk-domain-disputes/.
([43]) This is what happens in the case of EURid, which provides instructions on the conditions and procedure for disputing domain names through the Czech Arbitration Court or the WIPO Arbitration and Mediation Centre.
([44]) Nominet, Domain lock.
([45]) Domain name suspended or deleted for non-response to WHOIS enquiry; for further details, see the WHOIS Accuracy Program Specifications under ICANN's Accreditation Agreement.
([46]) Article 9 of the Danish registry terms and conditions.

- **Seized/blocked**: some registries have established rules to comply with court orders to seize or block a domain name upon notification ([47]). This entails that the disputed domain name may not be transferred, deleted or otherwise released as long as the order is in force. In practice, a registry can lock the DNS ([48]) or transfer its ownership to the law enforcement authority.

- **Terminated/cancelled**: a domain name can be terminated for a number of reasons, including a dispute resolution decision establishing abusive behaviour such as use in bad faith ([49]), non-fulfilment of eligibility criteria, or the breach of rules set out by the registry ([50]).

6. Good Practices and their Potential for Extension

Experts have identified a number of good practices to prevent the IP-infringing use of a domain in each stage of its life cycle.

6.1 Pre-registration

6.1.1 Terms and conditions

Several experts explained that good practice starts with the terms and conditions set by the registry. On top of the conditions applying to the registration of a domain, some registries also set conditions for its use. They usually detail the activities that would be considered a breach of the law and/or of contractual terms. It has been suggested that terms and conditions could clearly list IPR infringement as one of the breaches of contract that can lead to the suspension of domains. This is the case in the following examples.

- .**uk**: Nominet's terms and conditions prohibit, among other activities, the registration and use of .uk domains for unlawful purpose or to infringe intellectual property ([51]). In its 'criminal practices policy', Nominet provides a detailed description of how it works with selected UK law enforcement authorities when notified of illegal activities on a .uk domain ([52]).

([47]) Section 8 of the EURid Terms and Conditions, and Article 18, Regulation (EC) No 874/2004/EC.
([48]) See under paragraph 'Locked'.
([49]) ICANN's Uniform Domain Name Dispute Resolution Policy.
([50]) Article 12 of the EURid Registration Policy.
([51]) Nominet, Terms and conditions of domain name registration, Article 6.
([52]) Nominet, Criminal Practices Policy.

- **.hu**: Article 2(2)(1) of the Domain Registration Policy states that '[t]he Domain Applicant is free to choose the domain name to be delegated, within the framework of laws and the Policy, but the Domain Applicant shall act with utmost care in choosing the domain name so as the application, the domain name, and its usage shall not violate the rights of other persons or entities (e.g. the right of exclusive names, the right of privacy, the right of reverence, the right of intellectual property, etc.)'. In addition, it requires domain applicants to 'check the commercial register or major trademark databases before choosing the domain name' ([53]). The policy includes links to the Hungarian Intellectual Property Office's trade mark database and TMview ([54]) to facilitate verification.

- **.us**: .US has established an 'acceptable use policy' listing a series of uses of a.us domain for illegal purposes, including infringing 'the intellectual property rights of any other person or entity including, without limitation, counterfeiting, piracy or trademark or copyright infringement' ([55]). The policy details the different steps that the registry may take when a domain is used for illegal purposes, including disqualifying the registrant or its agent 'from making or maintaining any Registrations or Reservations in the usTLD if [they are] found to have repeatedly engaged in abusive registrations …'.

Specification 11 of ICANN's Registry Agreement also obliges Registry operators to include in their agreements with registrars 'a provision prohibiting Registered Name Holders from … piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name' ([56]).

Challenges and opportunities: some experts consider terms and conditions prohibiting the use of a domain name for IP-infringing activities a way to facilitate subsequent action and avoid any legal difficulties when enforcing these contractual terms. While the terms and conditions of registries often include provisions and mechanisms to deal with situations in which the name of a domain itself infringes IP, they do not typically include provisions on the use of the domain for IP-infringing activities, as this is the responsibility of the editor of the website.

([53]) .hu Domain Registration Policy, Article 2(1)(1).
([54]) TMview.
([55]) .US, usTLD Acceptable Use Policy, Articles 1 and 3.
([56]) ICANN, Registry Agreement, Specification 11, pp. 97-98.

Some experts explained that this reflects the position of most registries, that: '[t]he qualification of content as 'illegal' depends on the local legal framework and may even vary depending on the context. Whether content is illegal or not is a decision for local courts or competent authorities. […] A registry … does not have a special authority to effectively judge the legality of content that is put online' ([57]).

In this context, some registries have developed notice and takedown and/or trusted notifier mechanisms for relevant law enforcement authorities to notify them of illegal use (see section 4.3). Terms and conditions requiring registrants to check relevant trade mark databases, with links to search tools or databases (e.g. .hu or .uk) also constitute a way of avoiding bad-faith registration of domain names that potentially infringe trade mark rights.

6.1.2 Specific requirements on domain privacy and proxy services

ICANN discourages the use of privacy or proxy services. In particular, registrars and resellers must comply with the Specification on Privacy and Proxy Registrations and all other relevant obligations set forth in ICANN's Accreditation Agreement ([58]). Since 2016, ICANN has also been working on a privacy and proxy service provider accreditation program that is currently on hold ([59]). Some registries have developed specific policies with regard to privacy and proxy services.

- **.uk**: Nominet sets a number of conditions for the provision of proxy services, including:
  - registrants should not be misled into buying a proxy service 'by false claims … that a Proxy Service is required to protect their privacy';
  - accredited channel partners must inform Nominet of the proxy name and contact information that they will be using;
  - proxy service registrations 'must be opted in to the full public WHOIS'.
  - the registrar must promptly forward on to the registrant any correspondence received using the proxy service's contact information.

- **.us**: .US does not allow proxy or private registration, and 'enforces a registrar's obligation to not offer such services to .us domain name registrants'. It also uses 'an algorithm to detect the

([57]) CENTR policy document on domain names registries and online content, pp. 11-12.
([58]) ICANN, Registrar Accreditation Agreement.
([59]) ICANN Privacy and Proxy Services Accreditation.

inadvertent or intentional registration of proxy, anonymous and/or private domain name registrations …' ([60]).

- **.be**: DNS Belgium does not allow the use of privacy or proxy services if the aim is 'to shield the identity of the real domain name holder' ([61]).

Challenges and opportunities: since the entry into force of the GDPR, most European ccTLDs registries do not make data on individual registrants publicly available through their WHOIS service ([62]). This calls into question part of the rationale for individual users to use privacy or proxy services to register EU ccTLDs for legitimate purposes, and may be taken into account by EU ccTLDs registries when deciding whether and under what conditions to allow the use of such services. While some experts suggested that privacy and proxy services may still be used for legitimate purposes ([63]), other experts considered that they should not be allowed when the domain name is used for a website engaged in commercial activities or the collection of personal data.

6.1.3 Alert systems and rights protection mechanisms

Trademark Clearinghouse: with the rollout of new generic top-level domains, IP protection measures were put in place to 'enable trademark holders protect their rights during the DNS expansion'([64]). Trade mark holders pay a fee to record their rights information with the Clearinghouse, which provides this information to registries and registrars dealing with new gTLDs during the domain name registration process. This system gives trade mark owners access to different services.

- **Sunrise Services**: giving trade mark owners priority access to domain names associated with their trade marks in new gTLDs ([65]).

- **Trademark Claims services**: sending a registrant 'a warning notice when attempting to register a domain name that matches a trademark [registered with the Clearinghouse] ([66])'. If

([60]) .US FAQ, Will proxy registrations, sometimes called 'domain privacy' be allowed on my .US domain name.
([61]) Article 8(a)(6) of the terms & conditions for .be domain name registrations.
([62]) CENTR survey on Whois status and impacts from GDPR, October 2018, p. 3. It is important to note that there is a distinction between individual or legal entities registering EU ccTLDs, with almost half of registries continuing to publish registrant's contact details in their WHOIS service when the registrant is a legal entity.
([63]) One expert mentioned that proxy or privacy services may be used by journalists, whistleblowers or human rights advocates.
([64]) http://newgtlds.icann.org/en/about/trademark-clearinghouse
([65]) Trademark Clearinghouse, Sunrise services.

the domain name registrant continues the registration, the trade mark owner receives a notification.

- **Ongoing Notifications Service**: sending the registered trade mark owners a notification each time a domain name fully or partially matching their trade mark is activated ([67]).

Notifications to EU trade mark (EUTM) holders/applicants upon registration of .eu domain name: EURid and the EUIPO have developed a collaboration and put in place an 'alert system' for .eu domain names. This free service means 'holders and applicants of a[n] EUTM can opt-in to receive alerts as soon as a[n] .eu domain name is registered that is identical to their EUTM (application). By receiving such alert, EUTM holders are informed much faster and may take appropriate action much sooner' ([68]). As a part of the collaboration between EURid and the EUIPO, EUTM applicants can also check if their mark can be registered as an identical .eu domain name at the end of their application. This allows EUTM applicants 'to take action before any speculative and abusive registration might occur' ([69]).

Challenges and opportunities: with regard to Trademark Clearinghouse, it was suggested that these measures, as well as the information on verified trade mark records, could be used across all gTLDs ([70]). Trademark Clearinghouse recently announced the extension of its 'ongoing notification service' to the .com TLD ([71]).

As for the collaboration between EURid and EUIPO, a recent study commissioned by the European Commission on speculative and abusive domain registrations recommends 'extending the .eu Registry's collaboration in place with the EUIPO to Member States' trade mark offices by offering the measures of availability check and/or alert to their users as well' ([72]). Similar collaboration and alert systems could also be developed with EU ccTLD registries with regard to national trade marks.

([66]) Trademark Clearinghouse, Trademark Claims services.
([67]) Trademark Clearinghouse, Ongoing Notifications.
([68]) Trademark Clearinghouse, EURid and EUIPO strengthen their collaboration, May 2019.
([69]) European Commission, Study on evaluation of practices for combating speculative and abusive domain name registrations, July 2020, p. 5.
([70]) ICANN, Trademark Clearinghouse.
([71]) Trademark Clearinghouse, Ongoing Notifications Coverage expansion, August 2020.
([72]) European Commission, Study on evaluation of practices for combating speculative and abusive domain name registrations, July 2020, p. 97.

6.2 Registration

Experts pointed to the fact that online criminals, be it for IP crime or other online crimes, rarely use their real contact details. Since registries' terms and conditions usually require domain name holders to provide correct data upon registration as well as to keep this data up to date on a regular basis ([73]), verifying the data provided by the domain name holder can be a very effective way to block fraudulent registrations. This verification can be performed at different stages of a domain name's life cycle.

6.2.1 'Know Your Customer' (KYC) checks at domain registration

Experts pointed out the requirements put in place by a certain number of registries for registrants to verify their identities.

- **.dk**: the Danish registration system, implemented by DK Hostmaster, requires Danish individuals and companies to verify their identity using NemID, the Danish solution allowing its users to electronically identify themselves on the websites of government agencies or for online banking. Foreign registrants who do not have access to NemID are subject to a risk assessment. A high-risk registration requires the registrant to prove their identity immediately before the domain name is activated in the .dk zone. A low-risk registration requires the registrant to prove their identity within 30 days, while allowing use of the domain name instantly ([74]).

- **.no**: the Norwegian registry (Norid) requires domain name holders to be registered either in the Norwegian Central Coordinating Register for Legal Entities or in the National Registry, with a Norwegian national identity number and a Norwegian postal address for individuals ([75]). The registry operator regularly checks that this is effectively the case. If not, it automatically removes the relevant domain name ([76]). Norid also limits the number of domain names within the .no ccTLD that an organisation or a private individual can hold ([77]).

- **.ee**: the Estonian Internet Foundation (EIF) requires the registrant or their representative to sign the application submitted to the registrar by hand, in the presence of the registrar's

([73]) CENTR policy document, Domain name registries and online content, p. 18.
([74]) https://www.dk-hostmaster.dk/sites/default/files/2018-06/DIFOs%20kriminalitetsbekaempelse_EN.pdf
([75]) Norid, Domain name policy, in particular Section 5.
([76]) CENTR policy document, Domain names registries and online content, p. 19.
([77]) Norid, Domain name policy, Section 5.

representatives or using the Estonian electronic identification (eID) solutions. The EIF also accepts other eID solutions, including ID cards from Belgium, Latvia, Lithuania, or Finland, or eIDEAS-certified smart cards ([78]). Alternatively, it accepts payment of the registration service fee through a separate transfer from a bank or PayPal account opened in the name of the registrant or their representative as a way to verify their identities ([79]).

- **.pharmacy**: some domains can be reserved for certain types of activities, with specific KYC requirements in place. This is the case for the gTLD .pharmacy that was acquired from ICANN by the National Association of Boards of Pharmacy (NABP) ([80]). In order to register a .pharmacy domain name, the applicant/entity undergoes a review through the Pharmacy Verified Websites Program ([81]). This programme verifies that websites operating or doing business in Australia, Canada, Ireland, South Africa, Spain, the United Kingdom, the United States and other countries are properly licensed and follow applicable laws and business best practices. Once verified, the NABP approves the registration of the .pharmacy domain name, and adds it to its list of verified websites. It also allows the display in the web address of a 'seal' of safety that cannot be faked. The verification programme is recognised by a number of online advertising and payment services, which facilitates the use of such services by verified websites.

Challenges and opportunities: Some experts considered that KYC checks at domain registration through eID can be a very effective way to prevent fraudulent domain name registration with false identities and enhance trust and security in a given ccTLD. This also contributes to increasing the overall accuracy of the registrant data held by registries.

However, experts also highlighted that in some instances there are no eID solutions for all eligible registrants. In particular, they point to the absence of eID solutions for legal entities or for foreign individuals that may be eligible registrants. In this respect, ccTLD registries in the Czech Republic, Denmark, Estonia and the Netherlands are working on an EU-funded project to accept eID solutions

([78]) Estonian Internet Foundation, List of accepted electronic identification tools.
([79]) Estonian Internet Foundation, Domain regulation, Article 4.
([80]) The NABP is a non-profit organisation comprising state pharmacy regulators in the Bahamas, Canada and the United States.
([81]) .Pharmacy verified websites.

from all EU residents and 'allow registrants to secure their information on registered domain names through their national eIDs' ([82]).

When the use of eID solutions is not possible for some eligible registrants (e.g. legal entities or foreign individuals), some experts pointed to the possibility of using alternative identification solutions to reinforce KYC standards, such as performing a risk assessment on the registration data (as is done by DK Hostmaster), or verifying the registrant's identity through the payment method used to pay the registration fee (as is the case with the EIF) ([83]).

6.2.2 Monitoring to detect abusive registrations

Some experts pointed to the development of systems to detect abusive domain name registration applications in order to suspend them before delegation.

- **.eu**: EURid has developed its Abuse Prediction and Early Warning System (APEWS) to perform these checks. The system is trained with registration data, metadata and external intelligence ([84]). If the tool identifies a potentially abusive registration, its delegation in the .eu zone file is suspended ([85]) pending submission by the registrant of evidence that their registration data is correct. The final decision to proceed or not with the delegation is left to human review. Such a system can be amended to deal with specific crisis situations such as the COVID-19 pandemic ([86]), in which instance EURid implemented additional measures to verify registrants' data related to registrations containing COVID-related keywords to prevent abusive or speculative use. EURid also performs manual verification after delegation (see section 4.3).

- **.be**: DNS Belgium has deployed its Registrant Verification project, under which new registrations are automatically screened using a rule-based system that works on the basis of listed keywords, inconsistencies in telephone numbers, recognition of email addresses previously used for phishing campaigns, etc. If an incoming registration surpasses a set number of hit points, it is not delegated to the .be zone but instead redirected to an information

([82]) Connecting Europe Facility, Project 2019-EU-IA-0047.
([83]) When the registrant is a legal entity, one expert pointed to the importance of trying to identify the Ultimate Beneficial Owner (UBO).
([84]) Past cases of domain name registration abuse confirmed by experts.
([85]) EURid, APEWS.
([86]) EURid, COVID-19 and extraordinary measures on .eu domain names, April 2020.

page, and the registrant is required to provide documentary evidence proving their identity. The domain name will only be delegated once the registrant's identity has been verified. This project aims to deal specifically with potentially fraudulent registrations ([87]).

Challenges and opportunities: the automated detection of suspicious and potentially abusive registrations before delegation can be particularly effective when supported by advanced machine learning and artificial intelligence. 'In contrast to blacklists ([88]), which only offer protection after some harm has already been done, [such a] system can prevent domain names from being used before they can pose any threats ([89]).'

However, the development and maintenance of such a system requires significant resources and human supervision, and it needs to be constantly adapted, as criminals adjust their tactics to defeat automated detection. It may also need to be adapted to address specific situations (e.g. the COVID-19 pandemic). Automated detection must be complemented by human review to ensure the accuracy of the legal assessment and proportionality of the response mechanism in case of an infringement, which requires further resources. The effectiveness of such systems is limited when stolen individual or business details are used to fraudulently register a domain.

It has been suggested that further improvements to such systems could be made by harvesting more data regarding the registrants of the removed domains and further developing predictive models to identify high-risk applications. The work of EURid in that field has been pointed out as good practice ([90]). As cybercriminals often work across many TLDs, it would also be helpful if registry operators could develop ways to share data with each other so that patterns detected in one TLD could be used by other TLDs to determine whether similar illegal activities are ongoing, or could even be averted before cybercriminals start their activities in those TLDs.

([87]) DNS Belgium, DNS Belgium checks registration data even faster, November 2020.
([88]) Some experts suggested that blacklists developed by law enforcement authorities, trade authorities or consumer protection bodies could be taken into account for registries to consider taking down blacklisted domains and those domains whose activities are directly associated with blacklisted entities.
([89]) PREMADOMA: An operational solution for DNS registries to prevent malicious domain registrations, 2019, p. 1.
([90]) https://eurid.eu/da/nyheder/identification-of-malicious-dns/.

6.3 Post-registration

6.3.1 WHOIS verification after domain registration

Experts pointed to automated and manual verification of WHOIS contact details, with domains being suspended when the registrant cannot prove their identity, as a very effective measure. A number of proactive and/or reactive WHOIS verification mechanisms were identified.

Proactive WHOIS verification

- .**eu**: as well as monitoring to detect abusive registration before delegation (see section 4.2), EURid's legal department performs manual verification on a daily basis ([91]) for potentially abusive domain name registrations. These verifications are part of EURid's standard procedures, and are based on the analysis of the domain names itself, including the use of well-known trade marks, the analysis of registration data and metadata, as well as a keyword analysis of HTML content. The content analysis supports the detection of fake web shops or of websites selling counterfeits of well-known brands. It was reported that in October 2018, EURid withdrew over 36 000 .eu domain names that had been previously suspended due to non-eligible registration data ([92]).

- .**it**: 'The .it Registry, using machine-learning algorithms, carries out syntactic and semantical controls on specific fields of the registrant contacts (taxpayer code nationality code, registrants type) ([93]).' If it finds registration data that is obviously false or inconsistent, the .it Registry revokes the domain name.

- .**us**: the registry Neustar has developed an algorithm to search the entire usTLD database for proxy registrations that are prohibited under .usTLD's terms and conditions (see section 4.1). Neustar runs this algorithm on a frequent basis (at least once per month) to ensure no new proxy registrations have been added to the usTLD zone.' If such a proxy registration is detected, the relevant registrar is required to correct the WHOIS record with the accurate domain name information within 15 days, or else 'the registrations are deleted and the Registrar is found to be in breach of its agreement, potentially resulting in sanctions including, but not limited to, termination' ([94]).

([91]) During working days.
([92]) https://eurid.eu/en/news/suspended-dns-withdrawn/.
([93]) European Commission, Study on evaluation of practices for combating speculative and abusive domain name registrations, July 2020, p. 56.
([94]) usTLD Registration Management, Volume 1 – Technical capability, November 2018, p. 184.

Reactive WHOIS verification

Registries such as the *Association Française pour le Nommage Internet en Coopération* (the French Network Information Centre) (AFNIC), DNS Belgium, Nominet and the *Stichting Internet Domeinnaamregistratie Nederland* (Foundation for Internet Domain Name Registration in the Netherlands) (SIDN) have put in place special procedures to report potentially false or incorrect registrant information.

- **.fr**: AFNIC provides a verification request form ([95]) with which the eligibility of a registrant can be checked (i.e. whether the registrant has an address in one of the EU Member States), and the registrant can be contacted if the information provided is suspected to be unreliable (i.e. postal address, email and telephone number).

- **.nl**: a similar verification process is offered by the SIDN: provided there is good reason to believe that fraudulent activities are taking place, the SIDN can ask for evidence that the registration data is correct. If evidence is not provided within 5 days, the SIDN may delink the domain's nameservers, and ultimately may even cancel the registration ([96]).

Challenges and opportunities: experts highlighted the commitment of the European Commission to support '… efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN), in compliance with Union law, including the rules on data protection' ([97]). In this respect, experts consider WHOIS verifications performed proactively by a registry, or following a verification request, a very effective way of dealing with domain names used to infringe IP. The domain name holders for websites engaging in illegal activities rarely use their real contact details and would typically not react to a verification request. This leads to the suspension of the domain name(s). It can even be more efficient and less burdensome than requesting the deletion of single domains for IP-infringing activities, as failure to comply with one verification request may result in the deletion of all the domain names of a specific domain name holder.

([95]) https://www.afnic.fr/en/dispute-resolution/tools-and-procedures/verification-request-16.html (information retrieved on January 2020).
([96]) SIDN, Verification of registration data (information retrieved on 6 April 2020).
([97]) Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.

In addition, this approach does not involve any assessment of the legality of the content or service associated with the domain name by the registry. It is based on the contractual obligation of the domain name holders to provide correct data upon registration, and to keep this data up to date.

The limit of this approach is the use of fake or stolen identity documents by some criminals during verification procedures. Since most EU ccTLDs are open for registration by foreign individuals, it is difficult to check the authenticity of foreign ID documents, with most registries not questioning the authenticity of the documents provided. In this context, the .dk registration system, which asks for a selfie of the registrant to check the authenticity of the identity documents, is considered an example of good practice.

6.3.2 Notice and takedown (NTD)

Some experts explained that most registrars and registries do not take down domain names for illegal content such as IP infringements, considering that the infringements occur at the level of webhosting and not of domain names ([98]). The takedown of the domain is only considered if the name itself infringes an IP right, or on a basis of a court order.

This leads to a situation where in many instances IP owners have to litigate for the infringing domain name to be taken down. Although a number of courts have ultimately decided in favour of IP owners in requiring Domain Name Service providers to take action ([99]), such an approach is generally considered unsustainable for IP owners.

If some registrars or registries do take down domain names for illegal content (without a court order and on a voluntary basis), they need a solid legal basis (e.g. stemming from their terms and conditions) to avoid any liability claims in the case of a wrongful takedown. Experts pointed to several notice and takedown schemes.

([98]) This issue was considered in one recent German case (Bundesgerichtshof, I ZR 13/19, 15 October 2020).

([99]) The following cases were handed down in EU Member States (Belgium, Germany and Luxembourg): District Court Luxembourg, BEA v EuroDNS, 16 March 2016 (26 TPB domain names); District Court Luxembourg, BEA v EuroDNS, 22 February 2017 (6 domain names); Court of Appeal Cologne, 1API (The Pirate Bay), 31 August 2018; Court of Appeal Saarbrucken, KeySystems v Universal Music, 19 December 2018 (H33T); District Court Brussels, BAF v DNS.be, 23 August 2013 (spellen-ds.be, jeux-ds.be).

- **.uk**: in the Nominet takedown procedure, with the Police Intellectual Property Crime Unit (PIPCU), this Unit processes and coordinates requests to Nominet relating to IP infringements from nationwide sources ([100]).

- **.be**: a 'Notice & Action' protocol has been in place since December 2018 between the .be registry (DNS Belgium) and the Federal Public Service (FPS) Economy ([101]). Under this protocol, the Economic Inspection Department (a department of FPS Economy) can ask for a .be domain name to be suspended and redirected to a warning page within 1 working day. The protocol is limited to serious infringements of the economic legislation that harm consumers the most and are committed by persons or entities that are consciously violating the rules, and is employed when traditional legal means cannot be used effectively ([102]). Experts explained that this system requires two basic elements: a legal competence for the signing governmental entity to deal with breaches of the regulatory framework and a willingness to assume liability in the case of erroneous judgements ([103]). As part of this formalised cooperation, the FPS Economy also commits to intervene in case a registrant starts litigation ([104]).

- **.nl**: the SIDN established an NTD process ([105]) following the signing of the voluntary Dutch national NTD code of conduct ([106]). The complainant needs to provide evidence that sufficient steps have been taken to successively approach the content provider, the website manager, the registrant and the registrar of the domain name. The SIDN only takes action to prevent 'clearly unlawful or criminal activity'. If 'expert legal opinion is needed to decide whether an activity is unlawful or criminal', the SIDN does not take action. As part of the notification process, the complainant also has to agree that they will be financially responsible if the SIDN is sued for acting on the notification.

Challenges and opportunities: experts noted that the e-Commerce Directive encourages cooperation between stakeholders to reduce unlawful activity online, and that NTD procedures

([100]) https://media.nominet.uk/wp-content/uploads/2018/11/Tackling-online-criminal-activity-November-20181.pdf.
([101]) The Federal Public Service Economy is a government entity whose counterpart in other EU Member States would probably be called the Ministry of Economic Affairs. More information is available at https://economie.fgov.be.
([102]) DNS Belgium, Fraudulent websites offline within 24 hours as of 1st December, November 2018.
([103]) DNS Belgium, Notice & Action charter DNS Belgium/Belgian Government: joining forces in combat against e-commerce fraud, March 2019.
([104]) As the N&A cooperation between DNS Belgium and FPS Economy has proved to be successful, DNS Belgium is currently in negotiations with various governmental entities to conclude similar agreements.
([105]) SIDN, Complaining about the content of a website (information retrieved on January 2020)
([106]) https://noticeandtakedowncode.nl/wp-content/uploads/2018/12/NTD_Gedragscode_English.pdf.

contribute to reducing online criminal activities in general. However, some experts reiterated that registrars or registries do not host content and do not have the authority and in many instances the competence to make decisions on the legality of content hosted on domain names they are delegating (see section 4.1.1). They point to the consequences and risks of legal liability if a registry wrongfully takes down an entire domain. In this respect, they highlighted the need to set up notification systems for stakeholders who have the legal competence to determine whether a law has been infringed or not, and provide liability safeguards in case a registrant starts litigation to challenge the takedown of their domain.

Other experts suggested that, in some instances, a court decision ordering internet access providers to block access to a website could be enough to establish that its content is systematically illegal and provide the level of legal security needed for the registry of the associated domain name to voluntarily take action when notified of such decision. Such an approach should take into consideration the scope of the blocking order, as well as the jurisdiction and national regulation under which it was issued.

Experts also indicated that it is important for the functioning of notification mechanisms that the mechanisms allow notifications 'in bulk'. As new domain registrations for most top-level domains can go online within a few minutes, and fraudulent registrations are performed on a large scale, any effective measures against such registrations also need to allow takedowns 'in bulk'.

One opportunity outlined by an expert relates to the possible demotion of websites in search results based on the number of notifications for IP infringements. This metric could be used to affect the ranking of a website on a search engine in an attempt to draw attention away from infringing domain names.

6.3.3 Trusted notifier systems

Experts pointed to the approach taken by certain domain name registrars and registries that have established cooperation with IP owners and consider them trusted notifiers. If clear evidence is provided of unlawful activities occurring at a domain name, the relevant domain name registry or registrar can intervene voluntarily to make sure the abuse of the domain name ends. Experts highlighted two good practices in that respect, namely the 2016 Donuts([107]) and Radix([108]) agreements to treat the Motion Picture Association as a trusted notifier.

([107]) MPA, Donuts and MPAA establish new partnership to reduce online piracy, February 2016.

They also pointed to the pilot launched by the US Food and Drug Administration (FDA) and the National Telecommunications and Information Administration (NTIA), with Neustar, Verisign and the Public Interest Registry, to deal with the illegal availability of unapproved opioids online. Under this pilot, 'the FDA will notify internet registries that are participating in the pilot – Neustar, Verisign and Public Interest Registry – when the agency sends a warning letter to a website operator and the website operator does not respond adequately within the required timeframe. The internet registries will review the FDA's notifications and assess whether to take further voluntary action, including possible domain name suspensions or blocks' ([109]).

Challenges and opportunities: in support of trusted notifier systems, experts pointed to the Commission's communication on 'Tackling illegal content online' ([110]), which highlights the effectiveness of such systems in ensuring that illegal content is removed quickly and reliably. However, here again the challenge is to have trusted notifiers who are legally competent to determine if a law has been infringed or not and provide liability safeguards for the registry.

In this respect, some experts suggested that a reliable 'one-stop shop', cross-sectorial depository for registering trusted notifiers or flaggers could facilitate the notification process for all parties in all kinds of intermediary roles. Some experts pointed to the complexity of setting up such a one-stop shop at the European level, as a trusted notifier may have the legal competence to determine a law infringement under the legal framework of one EU Member State, but not of another.

6.3.4 Tools to contact domain name holder or request WHOIS information disclosure

Since the entry into force of the GDPR, personal data in the WHOIS allowing the identification of the domain name holder is in general no longer publicly available, which poses a new set of challenges. In this context, experts mentioned tools developed by the French registry AFNIC and the Belgian registry DNS Belgium that allow IP owners to contact a domain name holder by way of a contact

([108]) MPA, Radix and the MPAA establish new partnership to reduce online piracy, May 2016.
([109]) Federal government announces new pilot program to help stop illegal availability of unapproved opioids online, June 2020.
([110]) https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF (information retrieved on January 2020).

form that sends a message to the email address linked to the domain name in the registry ([111]). These experts suggested that such tools be considered good practice ([112]).

It is important to note that while the GDPR has had a significant impact in limiting the level of publicly available information through WHOIS, this does not prevent the registry or registrar from sharing registrants' contact data with third parties (such as IP owners) that can demonstrate a specific interest, for example the need to contact the registrant and ask for discontinuation of IP infringements, or to obtain a registrant's contact data in order to start formal legal proceedings.

In this respect, a number of European registries have put in place WHOIS disclosure forms ([113]).This is the case with DNS Belgium, which has made available a request form for disclosure of WHOIS contact data ([114]) that allows third parties (such as IP owners or their legal representatives) to retrieve registrants' contact data that is not available through the normal WHOIS tool. All such requests are reviewed by the Data Protection Officer (DPO) before any information is shared with the requester.

Challenges and opportunities: putting in place a contact form is relatively simple from a technical point of view and does not incur a significant cost. In addition, if the contact form returns an invalid email address for the registrant, this could be a strong indication that the registration data may not be accurate, and may trigger a WHOIS verification.

WHOIS information disclosure processes and forms that are compliant with the GDPR legal requirements can also be put in place, though specialised resources are needed to analyse and deal with such requests.

Some experts pointed to the fact that although such systems can be useful in some instances, disclosure decisions need to be based on clear standards balancing the interest of registrants against the need to '… [protect] the public from the harms associated with bad actors seeking to

([111]) https://www.afnic.fr/fr/resoudre-un-litige/actions-et-procedures/joindre-le-contact-administratif-d-un-domaine/.
([112]) This method is also under consideration in the context of ICANN's WHOIS policy development process; see https://gnso.icann.org/en/group-activities/active/gtld-registration-data-epdp-phase-2.
([113]) As part of this analysis, information on WHOIS disclosure processes was provided for 11 European ccTLDs, including .at, .be, .cz, .dk, .eu, .fr, .hr, .it, .lu, .nl, .pl, and .se.
([114]) DNS Belgium, Request form for personal data disclosure.

exploit the domain name system ([115])'. In this respect, they pointed to the recent statement from the Government Advisory Committee to ICANN, reacting to the most recent recommendations on setting up a disclosure system, which 'caution[s] against creating 'a fragmented system for providing access consisting of potentially thousands of distinct policies depending upon the registrar involved' noting that the 'lack of consistent policies to access non-public information causes delays' which may impede investigations and may permit potentially injurious conduct to continue to harm the public ([116])'.

6.4 Domain name suspension or termination

6.4.1 Appropriate action

Experts suggested that the nature of the appropriate action by registrars and registries could be an interesting issue for discussion. While injunctive relief usually results in an order to stop providing a service, this may not always be the most effective measure in relation to domain names. Several domain name codes are available, each of them resulting in a specific status ([117]).

One expert mentioned that disabling the domain but keeping it frozen during the remaining period of the registration is an effective strategy. If the transfer of the domain is also an option, this might not be scalable for high volumes of affected domain names.

In some cases (e.g. seized domains or notice and takedown schemes), it is also possible to put up a warning page on suspended domain names ([118]). This page can be used to inform consumers about the infringements previously taking place on the domain (see section 4.5).

([115]) ICANN GNSO, Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, July 2020, p. 122.
([116]) Ibid, p. 123.
([117]) https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en
([118]) Examples include the banner provided by Europol as part of the 'In Our Sites' operations, or the banner used for the .be NTD scheme (See Notice & Action charter DNS Belgium/Belgian Government: joining forces in combat against e-commerce fraud, slide 9).

6.4.2 Voluntary collaborations and sharing of intelligence

Voluntary collaborations between registries, rights holders and law enforcement authorities may help the collection of relevant information, provide guidance and expedite procedures to limit IP-infringing uses of domain names. Experts pointed to a number of good practices in this field.

- **.uk**: Nominet has developed a collaboration with UK law enforcement authorities that led to a change in its terms and conditions: a number of UK law enforcement authorities can notify Nominet that a specified .uk domain is used for criminal activities. The registry suspends the domain name within 48 hours, provided the issuance of a notice to both the registrant and registrar ([119]). A report of suspension activity is published annually ([120]).

- .**eu**: EURid has developed a collaboration with the International Anti-Counterfeiting Coalition (IACC) ([121]) aiming to limit fraudulent registrations. According to EURid, this collaboration is based on 'exchanging statistical data and trends pertaining to cybercrime, and committing to cooperate on projects designed to address the issue' of cybercrime, specifically counterfeiting and piracy, in the .eu and .ею domain name spaces. EURid also shares information on particular suspicious domain names with third party experts depending on the type of abuse. Amongst others, information is shared with the Anti Phishing Working Group (APWG.eu), Europol and the Centre for Cybersecurity Belgium.

IP owners can also share information on domains infringing their rights with law enforcement authorities through the EUIPO IP Enforcement Portal (IPEP) ([122]). Among the different functionalities it provides, IPEP allows IP owners to send alerts on online infringement of their rights on EU ccTLD domains. The online infringement alert form allows IP owners to fully document infringements of their rights ([123]). They can choose to share these alerts with enforcement authorities for this information to be included in their takedown operations. These alerts are also systematically shared with Europol.

Challenges and opportunities: with regard to the IPEP online infringement alert system, it may be interesting to explore if, beyond customs and police authorities, such alerts could be shared on a

([119]) Nominet, Nominet formalises approach to tackling criminal activity on .UK domains, April 2014.
([120]) Nominet, Tackling Online Criminal Activity, 1st November 2018 - 31st October 2019, November 2019.
([121]) EURid, EURid and IACC Team Up to Fight Cybercrime.
([122]) IP Enforcement Portal: the single platform to deal with IPR enforcement matters.
([123]) IPEP, Step-by-step user guide for rights holders, p. 89.

voluntary basis with other national authorities that have established collaborations with ccTLD registries to take down domains used for illegal activities in general and IP-infringing activities in particular.

6.5 Communication campaigns and resources

Experts mentioned that some ccTLD registries are developing information resources about online illegal activities. There are several ways in which registries inform their national communities, including meetings, workshops, presentations and webpages describing potential issues and dangers, registry policy and their role in dealing with the use of domain names for illegal activities.

- **.pt**: the Portuguese registry has entered into a collaboration with the General Inspectorate of Cultural Activities, associations representing copyright owners, telecom operators and the advertising industry. In this context, it has developed and hosts an online portal providing easy access to websites that offer IP-compliant digital content ([124]).

- **.fr**: the French registry provides a link to the Ministry of Internal Affairs' dedicated reporting platform, where illicit content or conduct can be reported ([125]). However, this reporting platform is not intended for reporting IP-infringing content or activities.

- **.uk**: Nominet provides users with information on how to contact the registrar or website owner if they want to object to website content, and with links to the relevant authorities' websites ([126]). In addition, if a domain name is suspended due to criminal activity, Nominet redirects 'web users to a secure site providing consumer advice and education for potential victims of sales of counterfeit branded goods' ([127]).

- **.no**: the Norwegian registry has published a guide for law enforcement authorities, police and others working in the judicial system ([128]).

([124]) APEL, 2014 (only available in Portuguese).
([125]) The French Ministry of Interior's webpage for reporting illegal content on the internet (only available in French).
([126]) Nominet, Complaints.
([127]) Nominet and PIPCU tackle cyber crime with launch of new landing pages for suspended criminal domains, November 2020.
([128]) Norid, Domain conflicts in the legal system.

- **.ch**: Switch has created guidelines for law enforcement authorities on how to request that a domain name be terminated or blocked as part of a criminal or administrative proceeding. The guidelines also provide details on how the registry might respond to their requests ([129]).

Challenges and opportunities: the development of such communication campaigns and resources offers clear opportunities to undermine the use of domain names for illegal activities, including IP-infringing activities. Some experts pointed to the need for IP owners and law enforcement authorities to explore with EU ccTLD registries the most relevant communication campaigns and resources that may be developed for specific IP-infringing uses of certain ccTLDs.

7. Conclusion

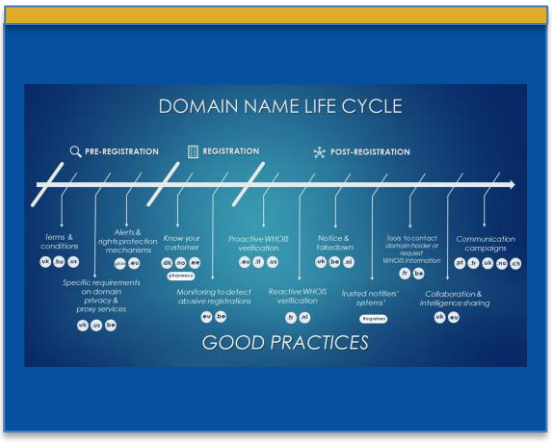
This discussion paper on domain names will hopefully contribute to a better understanding of the good practices that are developing to prevent the misuse of domain names for IP-infringing activities, and support IP owners in devising the best strategies to protect their rights. It will hopefully also contribute to the discussions on the challenges and opportunities to extend or replicate some of the good practices identified. The Observatory, with the support of its Expert Group on 'Cooperation with intermediaries,' is working on similar discussion papers on social media and payments, and will keep developing its work to cover a broad set of intermediaries.

([129]) Switch, Revocation and blocking of .ch domain names - Guidelines for authorities.

8. Glossary: Terms Used

Term	Abbreviation	Definition
Country code top-level domain	ccTLD	An internet top-level domain generally used or reserved for a country, sovereign state or dependent territory, identified with a country code (e.g. .dk, .fr, .eu).
Domain Name System	DNS	The global hierarchical system of domain names that turns machine-readable internet addresses into website names that people can understand.
e-identification	eID	The process of using personal identification data in electronic form, uniquely representing either a natural or legal person. This is one of the tools to ensure secure access to online services and to carry out safer electronic transactions .
European Union trade mark	EUTM	A trade mark for goods or services that is registered in accordance with Regulation (EU) 2017/1001 and is effective throughout the European Union.
Generic top-level domain	gTLD	One of the categories of top-level domains that do not correspond to any country code (e.g. .com, .net, .org).
Intellectual property	IP	Copyright and related rights and industrial law (trade marks, designs, patents, plant variety rights and geographical indications), and trade secrets.
Internet Corporation for Assigned Names and Numbers	ICANN	A non-profit organisation responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the internet.
IP Enforcement Portal	IPEP	The single EU platform to deal with IPR enforcement matters provided by the European Union Intellectual Property Office.

Term	Abbreviation	Definition
Know Your Customer	KYC	The process by which a service provider uses different means to verify the identity of a client before or after they start using its services (e.g. use of eID solutions).
Notice and takedown	NTD	The process put in place by an online intermediary by which users and authorities can report illegal content.
Top-level domain	TLD	Names at the top of the DNS naming hierarchy that appear in domain names as the string of letters following the last dot, such as '.net' in 'www.example.net'.
Uniform Domain Name Dispute Resolution Policy	UDRP	Under the ICANN UDRP, disputes over entitlement to a domain-name registration are ordinarily resolved by court litigation between the parties claiming rights to the registration. In disputes arising from registrations allegedly made abusively (such as cybersquatting and cyberpiracy), the ICANN UDRP provides an expedited administrative procedure to allow the dispute to be resolved without the cost and delays often encountered in court litigation.
WHOIS	WHOIS	Records containing registration information about registered domain names, as well as the protocol used for querying databases that store such records.



DOMAIN NAMES – Discussion paper on: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities

ISBN 978-92-9156-287-9 doi: 10.2814/238062 TB-02-21-137-EN-N