ICANN org Submission to the European Commission Call for Evidence on the EU Toolbox Against Counterfeiting

6 April 2022

Executive Summary

The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit, public-benefit corporation that, on behalf of the Internet community, among other functions, oversees the technical coordination of the top-most level of the Internet's Domain Name System (DNS), and especially its security, stability, and resiliency.

ICANN, through its multistakeholder governance model, brings together governments, non-commercial and commercial stakeholder groups, civil society, and individuals. Each group represents a different interest on the Internet. Collectively, they make up the ICANN community, which develops policies for the DNS through a consensus-driven, bottom-up process.

The ICANN organization (ICANN org) submits this contribution in response to the Call for Evidence by the European Commission to gather evidence to support the upcoming "EU Toolbox against counterfeiting," with the aim of highlighting ICANN's role in making and enforcing policies that apply globally to the DNS and, in particular, to gTLDs, and to provide information relevant to IP infringement.

1. ICANN's Mission

ICANN's mission is to coordinate and ensure the stable operation of the Internet's unique identifier systems, including the DNS. ICANN dedicates a significant portion of its work to ensuring a strong foundation for this activity globally. ICANN allocates global unallocated IP space to the regional Internet registries (RIRs), who then allocate it to local Internet registries (LIRs) or Internet service providers in their regions. The ICANN community – made up of members of technical, business, government, and civil society groups – help support the DNS by defining and helping to publicize DNS-related rules. Without ICANN's management of this unifying system known as the DNS, we wouldn't have a globally accessible Internet, where it is possible to find each other anywhere in the world without risk of confusion. The DNS is a centerpiece of the Internet infrastructure, providing the ability for anyone in the world to access services and applications online using a name instead of numbers. The continued resilience and security of the DNS is critical regardless of the situation, location, or any contingencies.

2. ICANN's Multistakeholder Structure and the Development of Consensus-Based Policy

ICANN is made up of three parts: the ICANN community, a volunteer-based, open collection of global stakeholders who work together through a bottom-up process to make policy recommendations and give advice within ICANN's mission and scope; the ICANN Board, which adopts the policy recommendations made by the ICANN community, which in turn, become ICANN policies; and the ICANN organization (ICANN org) that implements policy.

The ICANN Bylaws make it clear that ICANN should support broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet in the multistakeholder policy development process. To this end, ICANN supports a number of diverse, community-based structures that collectively make up the ICANN community and are organized into three Supporting Organizations and four Advisory Committees. Within each of their specific remits as defined in the Bylaws, the Supporting Organizations develop policy recommendations through documented, bottom-up, transparent processes. The Address Supporting Organization focuses on policy issues relating to the operation, assignment, and management of Internet addresses; the Country Code Names Supporting Organization is responsible for developing and recommending to the ICANN Board of Directors global policies relating to country-code top-level domains; and the Generic Names Supporting Organization (GNSO) is responsible for developing and recommending substantive gTLD policies to the Board.

In relation specifically to this Call for Evidence, it may be helpful to note that the GNSO consists of a number of stakeholder groups that include gTLD registry operators and registrars who are bound by their respective Registry Agreements (RA) (for gTLD registry operators) or ICANN's Registrar Accreditation Agreement (RAA) (for registrars); commercial interests represented through the business, intellectual property, and Internet service provider and Internet connectivity provider constituencies; and civil society, academic and other non-commercial interests represented through the non-commercial stakeholder group. Policy development within the GNSO is managed by the GNSO Council, which comprises elected representatives from all of these stakeholder groups, and three other members appointed by ICANN's Nominating Committee.

The four Advisory Committees provide advice to the Board and to the ICANN community on matters within ICANN's mission that may have an impact on various interests and issues. For example, Internet end-users (via the At-Large Advisory Committee); public policy and government concerns (via the Governmental Advisory Committee); the operation, administration, security, and integrity of the Internet's root server system (via the Root Server System Advisory Committee); and the security and integrity of the Internet's naming and address allocation systems (via the Security and Stability Advisory Committee).

All four Supporting Organizations and three Advisory Committees seek to make decisions by consensus. There are specific requirements, such as voting thresholds, which govern the Board's decision whether to adopt or ratify policy recommendations that are developed through community consensus.

For the purposes of this Call for Evidence, two additional fundamental characteristics of ICANN's multistakeholder, consensus-based policy development and advice model should be noted. First, ICANN's accountability and transparency obligations require that any policies under consideration by the Board and that substantially affect the Internet, or third parties must be published prior to any Board action, to allow the public a reasonable opportunity to provide the Board with input about the proposed policies.

Second, ICANN's contracts with gTLD registry operators and registrars include a specific obligation for these contracted parties to comply with all gTLD policies related to subject matter covered by their contracts that are developed by community consensus through the GNSO policy process, approved by a GNSO Council supermajority vote, and adopted by the Board. Typically, these are referred to as "consensus policies." Notably, the Board can only reject consensus policy recommendations through a vote of at least two-thirds of the Board, and only

on the basis that the recommendations are not in the best interests of ICANN or the ICANN community. Thus, in addition to their existing responsibilities and obligations as laid out in each RA and RAA, ICANN's contracted parties are also subject to consensus policies developed by the global multistakeholder community. One example of such a consensus policy that is relevant to trademark rights-holders is described further below.

3. Policies Concerning Generic Top-Level Domains

ICANN policy and contractual requirements govern the practices of gTLD domain name registries and registrars. This covers approximately 206 million domain names globally. The remaining names belong to country code TLD operators, which set their own policies.

ICANN policy and contractual requirements for gTLD registry operators and registrars operate alongside applicable laws and regulations. Thus, ICANN policies and contractual requirements can only be applied within the bounds of such applicable laws and regulations.

ICANN policies and contracts cannot modify or circumvent applicable laws. ICANN org does not enforce laws; this is a task for governments. Rather, ICANN org enforces its own agreements and consensus policies that are developed by the ICANN community.

Importantly, ICANN can only act within its limited remit. The ICANN Bylaws make clear that ICANN's role does not extend to the regulation of online content, nor beyond the activities specifically recognized in the Bylaws. The Bylaws recognize the following activities as falling within ICANN's limited mission: the allocation and assignment of names in the root zone of the DNS, and coordinating the development and implementation of policies for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, resilience, security, and stability of the DNS; the facilitation of the operation and evolution of the DNS root name server system; the coordination of the allocation and assignment of the top-most level of Internet Protocol numbers and Autonomous System numbers; and the collaboration with other bodies, as appropriate, to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations. The Bylaws specifically state that "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide…" outside the express scope of the activities described above.

While gTLD registries and registrars, as online intermediaries, may play a role in this area, activities specifically focused on online content are beyond ICANN's remit.

3.1 Registry and Registrar Abuse Obligations and ICANN Enforcement

ICANN org monitors the compliance with and enforces the obligations prescribed in the RA, RAA, and the consensus policies developed by the global multistakeholder community. ICANN-accredited registrars must enter into a template RAA with ICANN. Thus, all gTLD registrars are party to identical agreements with ICANN. By contrast, there are variations among the current Registry Agreements that gTLD registry operators have in place with ICANN because the approach to the contents of these agreements has evolved over time. Many (but not all) registry operators have signed onto the Base Registry Agreement. Each of the individual gTLD registry agreements is accessible on the ICANN website.

ICANN-accredited domain name registrars are subject to specific obligations to address abusive registrations of domain names, including reports of intellectual property (IP) infringement. Section 3.18 of the 2013 RAA requires registrars to maintain an abuse point of contact to

receive "reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity," and to "take reasonable and prompt steps to investigate and respond appropriately" to any reports of abuse. Section 3.18.2 requires each registrar to establish and maintain a dedicated abuse point of contact, monitored 24x7, to receive reports of illegal activity by law enforcement, consumer protection, quasi-governmental, or similar authorities. It also requires the review of well-founded reports of illegal activity submitted to these contacts within 24 hours by an individual who is empowered by the registrar to take necessary and appropriate action in response to the report.

Generic top-level domain registry operators are also subject to abuse obligations. Specification 6, Section 4.1 of the Base Registry Agreement requires each registry operator to provide to ICANN and publish on its websites contact information (including email, mailing address and primary contact) for handling inquiries related to malicious conduct in the TLD, and to provide ICANN with prompt notice of any changes to such contact details.

ICANN Contractual Compliance enforces these obligations through addressing complaints, registrar audits, and proactive monitoring. During the 12-month period of February 2021 – January 2022, ICANN Contractual Compliance received almost 3,100 complaints concerning registrars' abuse obligations. Of these, approximately 1,200 were identified by the complainant as involving copyright or trademark infringement. Details on how these types of complaints were resolved are available here. Finally, the most recent Contractual Compliance audit of registrars focused on compliance with DNS abuse obligations. Results of that audit are available here.

3.2 gTLD Domain Name Dispute-Resolution Mechanisms of Interest to Intellectual Property Holders

ICANN has implemented multiple dispute-resolution and rights-protection mechanisms of interest to IP rights holders. The most well-known, the Uniform Domain Name Dispute-Resolution Policy (UDRP), provides an expedited administrative proceeding that trademark rights-holders can initiate as an alternative to court proceedings by filing a complaint with an approved dispute-resolution service provider. The UDRP is a consensus policy that applies to disputes regarding domain names registered at the second level in all gTLDs, as provided in the RAA.

The UDRP is the oldest of the consensus policies developed through the ICANN multistakeholder model, having been approved in 1999. It was created to provide a quick, efficient, and cost-effective way to facilitate trademark protection at the second level of the DNS, through a mandatory online administrative proceeding that can precede or obviate the need for a court case (although it does not remove the option for either party to go to court if they wish). The remedy for a successful UDRP complaint is limited to either a transfer of the domain name to the complainant or a cancellation of the domain name.

Currently there are three UDRP providers: FORUM (based in North America), the Asian Domain Name Dispute Resolution Center (ADNDRC, based in Asia), and MFSD (based in Europe).

Where the UDRP applies to all gTLDs as a consensus policy, for the most recent gTLD expansion round, which was launched in 2012, ICANN also implemented a Uniform Rapid Suspension (URS) system and a Trademark Clearinghouse (TMCH) that offers additional protection to trademark holders in relation to these new gTLDs.

The TMCH is a system that facilitates certain rights-protection mechanisms in the gTLD namespace, specifically relating to the registration of second-level domain names (for example, enabling the provision of priority registrations for holders of TMCH-validated trademarks). The TMCH functions by authenticating information from rights holders from all over the world, maintaining a centralized database for verified trademarks, and providing this information to registries and registrars during the domain name registration process. The TMCH plays an important role in supporting ongoing protection of trademark rights in the domain name system.

The URS dispute resolution procedure is an online administrative proceeding that was based on the UDRP and designed to provide trademark owners with a quick and low-cost process to combat cybersquatting. The URS provides a single remedy of suspension of the domain name(s) at issue for the duration of the registration; unlike the UDRP, the domain name is not transferred to the complainant or otherwise canceled. Given the expeditious nature of a URS proceeding, the burden of proof is also higher than for a UDRP proceeding.

In the country code Top-Level Domain (ccTLD) environment, decisions as to whether to use the UDRP or some variation of it depends in part on the requirements of national law. For example, some ccTLD registries have adopted the UDRPs, while other ccTLDs use a modified version of the UDRP or have created a specific alternative dispute resolution procedure. The .eu registry, for example, has adopted an alternative dispute resolution procedure based on the dispute resolution principles included in the relevant EU Regulations about the .eu top-level domain. The procedure is managed by two providers, appointed by the registry, which act independently in a transparent and open manner.

3.3. Domain Name Registration Data Policy and the Impact of GDPR

In a hierarchical and decentralized system like the Internet, it is important for the entities that operate the pieces within it to be able to contact the other actors to warn of problems or coordinate responses to operational and other issues. Availability of registration data and access to it serves the public interest and contributes to the security and stability of the Internet by providing contact information to support efforts related to consumer protection, cybercrime investigation, DNS abuse, and intellectual property, and to address appropriate law enforcement needs. In that regard, the ICANN Bylaws mandate that there is a naming policy that makes certain data generally and publicly available: the so-called WHOIS or Registration Directory Services (RDS). Domain name registration data is a critical tool for identifying the actors behind domain names, which, in the context of counterfeiting, can be used to combat intellectual property fraud or prosecute trademark infringement. Domain name registration data includes personal directory-type information, such as a registrant's name, postal address, email address, and telephone number, as well as other, non-personal data, such as information about the domain name registrar.

The ICANN Bylaws provide that ICANN shall use commercially reasonable efforts to enforce its policies relating to the RDS and shall work with its Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to gTLD registration data, as well as consider safeguards for protecting such data. The Bylaws further recognize the need to ensure that ICANN's implementation of RDS requirements meets the legitimate needs of law enforcement, promoting consumer trust, and safeguarding registrant data.

Approximately 2,500 different legal entities around the world (the contracted parties) have their own subset of the global, decentralized RDS for gTLDs. There is no single, centralized database of this information; it is held by the individual contracted parties. The ccTLD

operators, which set their own RDS policies, have their own database for their respective ccTLDs. There are also RDS systems that cover IP addressing and other numbers, which set their own policies.

When GDPR was enacted, the ICANN Board adopted the Temporary Specification for gTLD Registration Data (Temporary Specification), establishing temporary requirements to allow ICANN and gTLD registry operators and registrars to comply with the GDPR while continuing to uphold existing ICANN contractual requirements and community-developed policies. It maintained robust collection of registration data, but restricted access to registration data that might include personal information. In effect, most directory information contained in gTLD domain registration data is no longer publicly available. Parties seeking access to non-public gTLD registration data must request that access from the contracted parties. Contracted parties are required to provide reasonable access to personal data in registration data based on a legitimate interest pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the registered name holder or data subject, pursuant to GDPR Article 6(1)(f). Each contracted party conducts its own assessment to determine whether a request for access will be granted. This has fragmented a system that many rely upon for reasons as varied as law enforcement investigations, intellectual property, and security incident response, among others. The new registration data policy recommended by the community, following the Temporary Specification, confirmed the Temporary Specification approach.

In addition, GDPR affected ICANN org's ability to investigate inaccuracy of registration data and take steps to address it with gTLD registrars. Pre-GDPR, ICANN org investigated the accuracy of gTLD registration data both in response to external complaints and in the context of the WHOIS Accuracy Reporting System project, in which ICANN org proactively identified potential inaccuracies and addressed them with registrars. This project was paused upon the effective date of the GDPR, given that much of the registrant contact information is now redacted from public view and, thus, not accessible for analysis. gTLD registrars remain obligated to collect, retain, and validate and verify this contact data, but are no longer obliged to publish it. Instead of this proactive analytic approach, ICANN org's activities in the registration data accuracy context are solely in the compliance context. If there is a question or complaint concerning a particular registrar's compliance with registration data verification and validation requirements, ICANN org will take steps to ensure the registrar is complying with the obligations in the RAA, according to which they must take reasonable steps to maintain the accuracy of their registrants' contact information.

4. DNS Security Threat Mitigation

How to address the malicious use of domain names, broadly referred to as DNS abuse, is one of the most important discussions for the ICANN community currently taking place, and ICANN is the right place to discuss issues related to technical abuse. However, depending on what is meant by DNS abuse, some types may not fall within ICANN's responsibility as the technical coordinator of the DNS. ICANN is not the Internet's content police.

ICANN org, consistent with ICANN's remit as defined by the ICANN Bylaws, focuses its DNS abuse-related efforts primarily on supporting the mitigation of DNS security threats, adhering to ICANN's technical role and capabilities.

ICANN org takes a multifaceted approach to supporting the mitigation of DNS security threats. DNS security threats include five broad categories of harmful activity: phishing, malware, botnet

command and control, pharming, and spam when used as a vector to deliver DNS security threats. Aside from monitoring the compliance with and enforcing the obligations prescribed in the RA, RAA, and the consensus policies as mentioned above, ICANN org is a trusted source of information about DNS threats by providing research, data, and expertise to help the Internet community have fact-based discussions about DNS abuse. ICANN provides tools to the Internet community to support mitigation of DNS security threats. Examples of ICANN's research projects and tools include:

- The **Domain Abuse Activity Reporting (DAAR)** system is designed to show where abuse is concentrated. The system collects DNS security threat data from reputation block lists (RBLs) for phishing, malware, botnet command and control domains, and spam as a delivery mechanism, and reports on what portion of domains in TLD zone files are reported in the RBLs on a daily basis via ICANN API monthly reports. Using DAAR data, ICANN recently published a report on DNS abuse. In contrast to many existing industry white papers and general discussions published on DNS abuse, this new report relies on four years of data. Typically, similar studies use data with a much shorter time span such as six months. As a result, the report demonstrates that when discussing DNS abuse trends in general, there should be caution because depending on the question asked, the data used, and the data timeframe, we will receive different results.

  We note that no one organization or data provider has a comprehensive overview of all security threats that exist on the Internet. Nonetheless, ICANN's DAAR datasets are a source of reliable and unbiased data and another source of possible research.

- The **Domain Name Security Threat Information Collection and Reporting (DNSTICR)** is an ongoing project of the ICANN Office of the Chief Technology Officer (OCTO) that looks at registrations related to specific events such as the COVID-19 pandemic or the conflict between Ukraine and Russia and aims to find evidence of any activity related to malware or phishing. Where sufficient evidence of malicious activity is found, ICANN org sends a report to the responsible registry or registrar so that they can determine the appropriate action, such as suspending or deleting the domain name.

In addition to these tools, registrars and registries have the ability to establish acceptable use and anti-abuse policies. These policies should include prohibitions on use of domain names to conduct or distribute DNS security threats, but also may contain further prohibitions that exceed the obligations in ICANN agreements or policies, such as content restrictions.

Furthermore, ICANN org maintains continued engagement with law enforcement, as well as with the cybersecurity industry, through organizations like the Forum of Incident Response and Security Teams (FIRST), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), the National Cyber Forensics and Training Alliance (NCFTA), and the Global Cyber Alliance. Also, ICANN org participates in closed, vetted trust-groups where actionable cyberthreat intelligence is shared, always keeping the focus on those threats that can put the security and stability of the DNS at risk, as well as on assisting the different security communities with subject matter expertise or with facilitation if needed to address the threats.

In terms of engagement, ICANN org has for years trained law enforcement and other public safety agencies on topics related to DNS investigations and will continue to do so. The org oftentimes partners with FIRST to deliver training to the incident response community, and with

the regional Internet registries (ARIN, APNIC, RIPE NCC, AFRINIC, and LACNIC) to deliver regional trainings that encompass both worlds, the names as well as the numbers.

Finally, ICANN org notes that normally, cyberthreat researchers who detect malicious domains not only share the relevant information with the cyberthreat intelligence community for mitigation and containment, but also frequently report the domains to the registrars or even the top-level domain operators in certain cases. Threat researchers may choose to follow this path regardless of whether the malicious domains use someone's trademark, the mimicking of that trademark being the lure to attract victims.

In cases like this, the fact that there is a likely trademark violation simply means that there is an additional path that may be followed on top of the reporting of the domain due to its involvement in activity like phishing, for example. That other path would normally be followed by lawyers, not threat researchers, and it would probably be under the UDRP or the URS, both of which are mentioned above.

5. Closing Remarks

ICANN org appreciates that protecting IP online can be challenging. As this high-level overview highlights, ICANN has several contractual and practical mechanisms to mitigate abuses such as IP infringement, while other actions remain outside of ICANN's remit. We would be pleased to discuss these mechanisms further with you, as well as ICANN's role in this space. ICANN org is also willing to share more concrete factual observations and data from the DAAR system, as well as the trends we observe in our engagement activities. ICANN org hopes this contribution will be helpful to support policymakers' analyses and objectives.