ICANN org Responses to the Public Consultation on the Digital Services Act package

(ICANN org responses are marked in blue – only the questions we are responding to have been copied here)

The document below represents only the questions deemed to be relevant for ICANN org. The full questionnaire is available here.

I. HOW TO EFFECTIVELY KEEP USERS SAFER ONLINE?

1. MAIN ISSUES AND EXPERIENCES

C. ACTIVITIES WHICH COULD CAUSE HARM BUT ARE NOT, IN THEMSELVES, ILLEGAL

4. In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain. (3000 character(s) maximum)

The Internet Corporation for Assigned Names and Numbers (ICANN) is the technical organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, i.e. the Internet's unique identifiers, ensuring the network's stable and secure operation. As a technical organization, it is not within our power, nor has it ever been intended to be within our mandate, to establish (il)legality of content. In that regard, the following answer concerns DNS-related abusive behavior, activities that leverage domain names and the global Domain Name System (DNS) for malicious purposes. Competent actors and public authorities determine whether such activities are harmful but not illegal, illegal, or some other legal classification.

Regrettably, and despite ICANN Org's swift and multifaceted response to DNS Abuse, in parallel with the global pandemic there has been a surge of online threats leveraging COVID-19 to further victimize vulnerable populations. As it has been widely reported, bad actors are taking advantage of the global COVID-19 pandemic by launching malicious online campaigns. Such malicious activities use or leverage domain names and the Domain Name System; there have been numerous reports of spikes in the use of COVID-19-related domain names for DNS abuse. These threats include phishing, business email compromise, malware distribution, scams, and many other types of attacks , ranging from fake web shops, credit card skimming and illicit pharmacies to ransomware .

It must nevertheless be underlined that, in our experience, this is not per se an increase in malicious online activities, but rather a movement from already known *attack vectors to* , or a combination with, *COVID-19-related attack vectors.*

5. What good practices can you point to in tackling such harmful activities since the outbreak of COVID-19? (3000 character(s) maximum)

Given the global nature of the Internet, the variety of actors involved and the multitude of jurisdictions, collaboration at the global level involving all stakeholders is required.

In response to the COVID-19 outbreak, various groups were formed to share valuable threat information, focused on the response to the pandemic in the cyber realm. ICANN org joined both the COVID-19 Cyber Threat Coalition (CTC) and the COVID-19 Cyber Threat Intelligence League (CTI League) along with hundreds of researchers from private companies and law enforcement officers from several countries. Similar work was undertaken by the incident response community through its existing Forum of Incident Response and Security Teams (FIRST) and by the threat research and operational security communities through the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), the Anti-Phishing Working Group (APWG), and the National Cyber-Forensics and Training Alliance (NCFTA). ICANN primarily contributes to these groups by providing subject-matter expertise and facilitating communication between the various parties interested in mitigating DNS abuse.

When it comes to mitigating DNS abuse as such, the ICANN org Security, Stability, and Resiliency team has built a system that helps identify abusive domains leveraging the coronavirus pandemic. This system looks for domain names similar to or incorporating terms such as “coronavirus”, “covid”, “pandemic”, “ncov,” and others, and once identified, assesses them against multiple high-confidence threat intelligence sources to determine whether or not they are involved in phishing and/or malware distribution. If so, the domain names and the data collected by the system will be shared with parties (such as registrars and registries) who are in a position to take action to disable unique identifiers, when action to disable unique identifiers is legally justified. In some cases, this may involve national and international law enforcement organizations. The system is being tested to ensure the highest confidence levels and to avoid false positives as much as possible. In addition, we’re working with a number of community members to ensure that the reports generated by the system meet their reporting requirements so that appropriate, legally justified, and timely action can be taken.

ICANN-accredited gTLD registrars, gTLD registry operators, and ccTLD registry operators have also taken actions aimed at helping to mitigate and minimize the abusive domain names being used to maliciously take advantage of the coronavirus pandemic, including engaging with the aforementioned groups and, where necessary, with public authorities. The ICANN Registrar Stakeholder Group has posted a useful guide, entitled “Registrar approaches to the COVID-19 Crisis,” which provides a number of steps and resources the *registrar community can use in their efforts. We'd like to also highlight this as a good practice in this context.*

D. EXPERIENCES AND DATA ON ERRONEOUS REMOVALS

11. Do you use WHOIS information about the registration of domain names and related information? (select one of the three options)

- Yes X
- No
- I don't know

12. Please specify for what specific purpose and if the information available to you is sufficient, in your opinion? (3000 character(s) maximum)

Registration data directory services, such as WHOIS, provide access to critical data related to the registration and usage of Domain Names and IP Addresses. This data enables ICANN and others to fix system problems and to maintain the stability of the Internet. It is indispensable to the smooth operation of the DNS, such as contacting network administrators for resolution of technical matters related to networks associated with a domain name or IP address (e.g., DNS or routing matter, origin and path analysis of a denial of service (DoS) attack and for other network-based attacks), to diagnose registration difficulties, or to contact web administrators for the resolution of technical matters associated with a domain name.

In addition, WHOIS, serves the public interest and contributes to the security 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. Domain name registration data can be used to determine domain name availability, combat spam and fraud, prosecute trademark infringement, and enhance the accountability of domain name registrants.

ICANN's mission to ensure the security and stability of the Internet's system of unique identifiers is reflected in the ICANN Bylaws, which recognize the need to ensure that ICANN's implementation of WHOIS requirements meets the legitimate needs of law enforcement, promoting consumer trust, and safeguarding registrant data.

The ICANN requirements for the contracted parties' public display of registration data have significantly changed, as part of ICANN's and ICANN's community efforts to bring the requirements into compliance with the GDPR. Prior to the adoption of the GDPR, the contracted parties were required to publicly display contact information for domain name registrants by default unless the registrant had taken steps to shield that data from public access, for example, by utilizing a privacy domain name registration service. Now, 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 on the basis of 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.*

13. How valuable is this information for you? Please rate from 1 star (not particularly important) to 5 (extremely important)

5 stars.

14. Do you use or are you aware of alternative sources of such data? Please explain. (3000 character(s) maximum)

No.

2. CLARIFYING RESPONSIBILITIES FOR ONLINE PLATFORMS AND OTHER DIGITAL SERVICES

8. What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.?

From the ICANN context, it is important that those writing legislation understand that a DNS service does not host or have visibility into content. The DNS should be seen more in the light of a directory service allowing users to find their way to the servers hosting that content.

As such, the suspension of a domain name may remove that referral, or those directions, but it does not, and cannot, remove the content.

ICANN addresses malicious activity online via contractual obligations with its registries and registrars, which include the obligation to investigate and report abuse. ICANN's Registrar Accreditation Agreement includes the obligation by registrars to maintain an abuse contact to receive reports of abuse, and an email address to receive such reports. Registrars shall also take reasonable steps to investigate and respond appropriately to any reports of abuse and maintain a dedicated abuse point of contact to receive reports of illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated by the government of the jurisdiction in which the registrar is established or maintains a physical office. Notices and reports of abuse and illegal activity need to be precise *and clearly identify the claims of illegal activity and applicable legislation. In some cases, such claims are too broad or vague for registrars to investigate and respond where disclosure would cause subsequent issues under global data protection laws .*

Registrars also sometimes receive complaints of abuse or illegal activity, where the complainant has not identified themselves or provided contact details, making it difficult to follow up or validate the claims. Registrars don't exert any control over the content of a website and cannot take down content hosted on a website. They can only suspend or terminate a specific domain name registration, but the website can in some cases continue to be accessed via an alternative domain name, a proxy or directly via the IP address. Suspending or terminating a domain name requires a diligent process to ensure false takedown requests do not impinge on fundamental rights such as freedom of speech or the freedom to conduct a business.

Takedown or suspension requests can also lead to problems related to jurisdiction and conflict of laws. Some registrars receive complaints that are specific to the laws of a particular jurisdiction, which the registrar may not be subject to, and which may conflict with laws in the jurisdictions that apply to them.

The Digital Services Act should be very clear in specifying its territorial applicability and address conflicts of laws with other jurisdictions. Registrars or ICANN cannot suspend access to a domain name in one region and leave access open in another to resolve such jurisdictional conflicts which would not appear expedient at times when proxies and VPN servers are becoming more and more widespread .

Combatting abuse requires predictable and reliable access to domain name registration data for those with a legitimate interest, which is where the WHOIS function is an important facilitator. The lack of access to WHOIS - a direct result of the redaction of personal data in the publicly available WHOIS records - has increased the administrative burden for law enforcement and cybersecurity agencies, hampering their efforts to identify and remove illegal content in a timely manner and engage registrars where required. Institutions with the experience and legitimacy to police illegal activity and to address jurisdictional disputes and conflicts of law is the most appropriate solution.

II. REVIEWING THE LIABILITY REGIME OF DIGITAL SERVICES ACTING AS INTERMEDIARIES?

2. The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain.

5000 character(s) maximum

In today's Internet, the functions and roles of intermediaries have become more diverse, and it is important to recognize the ability of each intermediary to play a role in this ecosystem. DNS services carry out a different function from web hosts. A company offering domain name registrations has no knowledge of the contents of the website that they are registering, but merely ensures that the global internet "address book" – the DNS – gets a user to the correct website when they type in a domain name. A web host, meanwhile, may act as a repository for important files that enable the functioning of a website, but rarely all the content of a website, which may be distributed across a variety of cloud providers and data centers. It is important for policy makers to make a careful assessment of which categories of intermediaries have enough visibility and control of services to make a monitoring obligation proportionate and effective. Failure to strike the right balance could hamper the functioning of the open and interoperable Internet, jeopardize net neutrality and endanger the freedom of information . For providers such as registrars and DNS services, robust mechanisms are in place to enable suspension or termination of a specific domain name registration when this is legally justified. From a legislative standpoint, it is critical that these functions don't become conflated with intermediaries with a greater degree of control over the data and content. It is also critical not to conflate the Internet's core infrastructure and operations with the applications that run on top of that infrastructure.

Similar to the GDPR, future EU legal acts addressing such digital intermediary services should follow the principle of 'technology neutrality' and openness to the future to ensure that future technological developments are not obstructed from the outset. Liability regimes that lack legislative clarity or are overly comprehensive risk standing in the way of economic progress and endangering the innovative spirit of small and large intermediary service providers alike. Providers which are primarily engaged in maintaining stability and interconnectivity should not be held responsible for any content from third parties which is beyond their control.