Framework to Address Abuse

The Domain Name System (DNS) serves as a crucial but largely unheralded system underpinning the Internet's ability to connect its users and devices. The safe and secure operation of the DNS has provided a firm foundation for the growth of the Internet as a global public resource, but much like the Internet as a whole, it is not immune to abuse. For the good of the Internet and everything it enhances, the undersigned domain name registrars and registries aim to reinforce the safety and security of the DNS by highlighting shared practices toward disrupting abuse of the DNS (DNS Abuse). A collection of governments worldwide, known as the ICANN Government Advisory Committee,[1] recently stated:

> Protecting the public from security threats and DNS Abuse is an important public policy issue …. If the public is to trust and rely upon the Internet for communications and transactions, those tasked with administering the DNS infrastructure must take steps to ensure that this public resource is safe and secure.[2]

The undersigned registrars and registries agree. Before DNS Abuse can be effectively addressed, we recognize the need for a shared understanding as how to define it. Leveraging our collective DNS expertise, relationships with law enforcement, governments and civil society, and knowledge of internet infrastructure, we offer the definition of "DNS Abuse" below, which registrars and registries should feel compelled to act upon. Further, we believe there are other forms of abuse that fall outside this definition of DNS Abuse, but that a registry or registrar *should* nonetheless take steps to address. We provide these definitions and practices in hopes of meeting two goals: (1) contributing to and encouraging the dialogue within our multistakeholder community, and (2) promoting DNS safety and security by disrupting abuse in, with, and around the DNS.

DNS Abuse

DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse). The Internet and Jurisdiction Policy Network's *Operational Approaches, Norms, Criteria, Mechanisms* provides the following definitions for each of these activities:

> **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.[3]

---

1 The GAC is an advisory body to the Internet Corporation for Assigned Names and Numbers (ICANN), the organization that oversees the DNS.

2 Government Advisory Committee Statement on DNS Abuse, 18 September 2019, https://gac.icann.org/contentMigrated/gac-statement-on-dns-abuse.

3 Internet and Jurisdiction, Domains and Jurisdiction: Operational Approaches, Norms, Criteria, Mechanisms (2019) ("I&J Operational Approaches"), page 20 at https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf; See M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), at

> **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.[4]
>
> **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.[5]
>
> **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to [the attacker's] site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.[6]
>
> **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.[7]

While Spam alone is not DNS Abuse, we include it in the five key forms of DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse. In other words, generic unsolicited e-mail alone does not constitute DNS Abuse, but it would constitute DNS Abuse if that e-mail is part of a phishing scheme.

We believe registrars and registries *must* act upon these categories of DNS Abuse. We are required by our agreements with ICANN to maintain abuse contacts (and preferably a webform) to receive abuse complaints and to promptly investigate allegations of DNS Abuse in good faith. In addition, each of the undersigned disrupts DNS Abuse when identified within our registrations and encourages others to do the same. That said, because of its role in the DNS, the only mitigation tool a registry or registrar[8] possesses is to disable the **entire** domain name. Registries and registrars do **not** have the ability to surgically target the "abusive parts" of a domain name or a particular

---

https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety-Net_Brochure-web2-2015-06.pdf;

4 I&J Operational Approaches at 20; See "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, at: https://niccs.us-cert.gov/about-niccs/glossary#B

5 I&J Operational Approaches at 20.

6 *Id.*; see Entries for DNS hijacking and DNS poisoning in the Kaspersky Lab Encyclopedia, at https://encyclopedia.kaspersky.com/glossary/dns-hijacking/

7 I&J Operational Approaches at 20; *see* "The Definition of Spam" by The Spamhaus Project, at https://www.spamhaus.org/consumer/definition/

8 Some (not all) registrars also act as hosting providers. Hosting providers do have the ability to remove specific content without acting at the DNS level. For purposes of this discussion, we examine only the registrar's ability to act in the capacity as a registrar, utilizing the DNS.

page on that domain. Unfortunately, disabling a domain name is as powerful as it is imprecise, especially when the DNS Abuse occurs on a broader platform, forum, marketplace, or other domain shared by large audiences.

Website Content Abuse

Registrars and registries frequently receive complaints for abuse that fall outside of DNS Abuse. These complaints most often focus on a website's content, or "Website Content Abuse." As registrars and registries, we are not required under our agreements with ICANN to monitor or suspend domains based on Website Content Abuse. Registries and registrars steadfastly maintain that this distinction is critical in order for the Internet to remain open for free expression. The line between free expression and illegal content varies across jurisdictions, cultures and even changes over time. A universally accepted global standard for evaluating content is not possible, nor is it ICANN's remit to create international online-content regulations.

Disproportionality and Collateral Damage

Moreover, acting at the DNS level to address Website Content Abuse in general is a disproportionate remedy that can cause significant collateral damage. For example, if a registry or registrar receives a complaint about specific content from a popular and otherwise legitimate website (e.g., movie fan forums or website builders), it cannot remove that specific content without disabling the rest of the domain (including any third-level domains, associated emails and legitimate content).

When Should a Registrar or Registry Act on Website Content Abuse?

Despite the fact that registrars and registries have only one blunt and disproportionate tool to address Website Content Abuse, we believe there are certain forms of Website Content Abuse that are so egregious that the contracted party *should* act when provided with specific and credible notice. Specifically, even without a court order,[9] we believe a registry or registrar should act to disrupt the following forms of Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking;[10] and (4) specific and credible incitements to violence. Underlying these Website Content Abuses is the physical and often irreversible threat to human life. Additionally, each registrar and registry has its own acceptable use policies or terms of use that set forth provisions that may cover these and additional forms of Website Content Abuses.

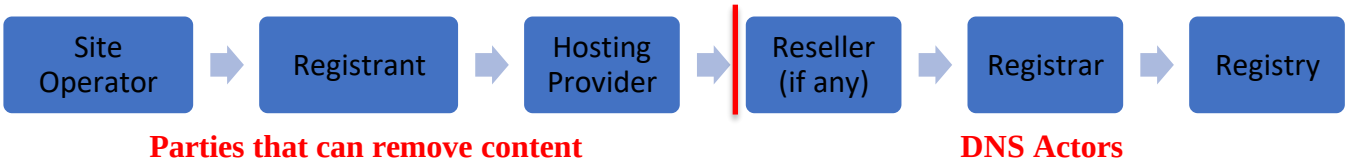
Proper Referral Procedures for Website Content Abuse

Because a registry and registrar cannot remove or alter website content, the most direct (and appropriate) path to resolving complaints about Website Content Abuse is shown below.

---

9 Registrars and registries also frequently receive orders from courts of proper jurisdiction which compel us to act upon domain names based on the website content.

10 "What is Human Trafficking?," United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html.



On this scale,[11] a complainant should exhaust its remedies with the "Parties that can remove content" before it escalates to the reseller (if any), the registrar, and the registry (in that order). The left side of the scale shows where Website Content Abuse can be more precisely addressed as these operators should have the ability to remove content without interrupting service for an entire domain name.[12] Because a registry or registrar can only disable an entire domain name, we must balance the harm faced by a complainant with potential harm to the registrant **and** also against harm to other, potentially valid and possibly critical uses of the domain name. A complainant should work first with the site operator, registrant or hosting provider to remove the content, rather than causing potential collateral damage by acting via the DNS.

What "Taking Action" Looks Like

Registrars and registries should promptly investigate allegations of DNS Abuse and the Website Content Abuse that falls within this framework. This requires coordination and good faith cooperation between the registrar and registry to balance the potential harm from the remedy against the harm caused by the abuse. When a registry identifies abuse, it should always provide notice to the registrar, given the registrar's closer business or contractual relationship with the registrant. This relationship allows the registrar to work with its customer to address the abuse, provide mitigating information, or, in the case of a compromised domain (where a registrant's credentials are compromised and the domain is put to abusive purposes without the registrant's consent or knowledge) to reinstate the domain to its prior, unabused state.[13]

The Role of Trusted Notifiers

Registrars and registries may wish to consider using subject matter experts, often called "Trusted Notifiers," to monitor and help address some of the categories of Website Content Abuse identified above, or other sorts of abuse that may fall under an organization's policies. Trusted Notifiers are more than an abuse referral service. Befitting their designation, Trusted Notifiers earn the registries' and registrars' trust with a recognized subject matter expertise, an established reputation for accuracy, and a documented relationship with and defined process for notifying the registries and registrars of alleged abuse. While it is ultimately the responsibility of the registries and

---

11 I&J Operational Approaches at 25.

12 Not all hosts and infrastructure providers can access specific content and in certain cases, they too can only shut down an entire site or customer account. That is why it is always most efficient to go as far left on the scale as possible to seek relief.

13 There are other options available that are not nearly as effective. A registry, for example, can delete a domain name, but that would allow the same potential bad actor to re-register the domain and engage in the same behavior. Similarly, transferring or redirecting domain names to combat abuse, while possible, would require court orders to be effectuated. See "Framework for Registry Operator to respond to Security Threats," (2016), https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en.

registrars to take action on verified forms of abuse, Trusted Notifiers can serve as a crucial resource to enhance the abuse monitoring and disruption procedures of registries and registrars.

ICANN's Role

Section 1.1 of ICANN's Bylaws states that ICANN is charged with ensuring the stable and secure operation of the Internet's unique identifier systems. It does that in several ways. ICANN relies on the tech community to review policy and other decisions for potential security and stability issues. Its Technology Office monitors gTLD zone files for DNS Abuse and reports on that abuse. ICANN contracts with registries and registrars to, respectively, monitor and address DNS Abuse to ensure that registries and registrars actively participate in this function and it enforces those contracts through its Compliance Office.

While ICANN plays an important role in mitigation of DNS Abuse, it has consistently made clear that it is not a regulator of website content. In fact, ICANN's Bylaws prohibit it from "regulat[ing] (i.e., impose[ing] rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide."[14] Further to that point, ICANN has stated that it is not:

> responsible for making factual and legal determinations as to whether content violates the law. ICANN cannot be put in the position of requiring suspension of domain names on the basis of allegations of blasphemy, hate speech, holocaust denial, political organizing, full or partial nudity or a host of other content that may be illegal somewhere in the world. That would be inconsistent with ICANN's mission, ICANN's limited remit and ICANN's responsibility to operate in accordance with a consensus-driven multistakeholder model.[15]

Although ICANN does not have the authority to regulate activities that fall outside of its clearly defined mission, it does serve an important role in contributing to multistakeholder community efforts by providing a discussion forum during its meetings and the opportunity to engage broadly within the community. The undersigned registrars and registries welcome the continued dialogue on this issue in hopes of raising the bar for responsible and thoughtful stewardship of the DNS.

Conclusion

We hope that this document will facilitate a productive conversation that moves the multistakeholder community forward towards a shared understanding of DNS Abuse and Website Content Abuse and the roles registrars and registries serve in addressing them. The authors of this document are committed to bettering the DNS by making it a more trusted space and encourage other contracted parties and the community to join us in these efforts.

---

14 ICANN Bylaws Article 1, Section 1.1(c) https://www.icann.org/resources/pages/governance/bylaws-en

15 ICANN is not the Content Police, June 2015, available at https://www.icann.org/news/blog/icann-is-not-the-internet-content-police; see also "About Website Content (2013), https://www.icann.org/resources/pages/content-2013-05-03-en ("complaints about website content are outside of ICANN's scope and authority").