Damming a river to catch a fish

Why the DNS must enable expression – not silence it

ARTICLE 19

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement, locally and globally, to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our nine regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on five key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

info@article19.org
www.article19.org
@article19org
@article19
@article19.bsky.social
facebook.com/ARTICLE19org/

© ARTICLE 19, 2026

This work is provided under the Creative Commons Attribution-Noncommercial-ShareAlike 4.0 licence. You are free to copy, distribute, and display this work and to make derivative works, provided you: 1) give credit to ARTICLE 19; 2) do not use this work for commercial purposes; 3) distribute any works derived from this publication under a licence identical to this one.

To access the full legal text of this licence, please visit: https://creativecommons.org/licenses/by-nc-sa/4.0/

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used. ARTICLE 19 bears the sole responsibility for the content of the document.

This report has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of ARTICLE 19 and can under no circumstances be regarded as reflecting the position of the European Union.

Co-funded by the European Union

AGILE advancing media resilience

Contents

Abbreviations

BAJ	Belarusian Association of Journalists
ccTLD	country-code top-level domains
CENTR	Council of European National Top-Level Domain Registries
CPC	Consumer Protection Cooperation
CSAM	child sexual abuse material
DNS	domain name system
DSA	Digital Services Act
EIA	Environment Impact Assessment
gTLD	generic top-level domains
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ISOC	Internet Society
MiCA	Markets in Crypto-Assets
OONI	Observatory of Network Interference
PDP	policy development process
PIR	Public Interest Registry
UDRP	Uniform Domain Name Dispute Resolution Policy
VPN	virtual private network

Acknowledgements

- Alissa Starzak, Cloudflare
- Andrés Azpúrua, VE Sin Filtro
- Ann Morton, Internet Infrastructure Coalition (i2Coalition)
- Ann-Cathrin Marcussen, Norid
- Belarusian Association of Journalists
- Blacknight Internet Solutions Ltd
- Bruce Tonkin, .au Domain Administration Limited (auDA)
- Christian Dawson, Internet Infrastructure Coalition (i2Coalition)
- Clara Ludvigsson, Internetstiftelsen (Swedish Internet Foundation)
- Declan McDermott, .ie
- Diego Ernesto Luna Quevedo, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia
- DotAsia
- Erick Iriarte Ahon, IALaw
- Francis Amaning
- Gurshabad Grover
- Hilde Thunem, Norid
- Jo-Fan Yu, Taiwan Network Information Center (TWNIC)
- Kristian Ørmen, Internetstiftelsen (Swedish Internet Foundation)
- Kwaku Antwi
- Let India Breathe
- Margarita Valdés, NIC Chile
- Mart van Santen, Greenhost
- Metaregistrar BV
- Non-Commercial Stakeholder Group (NCSG)
- Patrick Day, Cloudflare
- Polina Malaja
- Public Interest Registry
- Punktum dk
- Sarah Wyld, Tucows Domains
- Suzanne van Geuns, University of Wisconsin, Madison
- There Is No Earth B
- Thiago Ayub, Sage Networks
- Thiago Dal-Toe, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia
- Wisdom Donkor

1

Introduction

Content moderation is often associated with social media posts being blocked or taken down due to decisions by governments and social media companies. But government censorship tactics are increasingly moving into deeper layers of the internet stack. Beyond social media companies, infrastructure providers – such as those operating the Domain Name System (DNS), the 'address book' of the internet – also act as gatekeepers to content.[1] **When such tactics are applied to the DNS, the impact on freedom of expression can be devastating.**

Domain names are key for locating a particular webpage. The DNS translates website addresses (domain names, like 'article19.org') into internet protocol addresses (numerical labels that indicate where in the network a given website is located), so that the right page appears. The Internet Corporation for Assigned Names and Numbers (ICANN), a multistakeholder organisation, maintains the DNS.

ICANN policies are implemented by **domain operators**.[2] Domain name operators include:

- **Registries**, which manage domain name databases for top-level domains (such as '.com', '.uk', or '.org'), and
- **Registrars**, which liaise between registries and domain owners, known as **registrants**.

There are two types of registries:

- **ccTLDs** (those that operate country-code top-level domains, such as '.br' for Brazil)
- **gTLDs** (generic top-level domains such as .com or .music)

When a domain is suspended, *all webpages using the same domain can no longer be accessed.* This approach is equivalent to damming a river to catch a few fish. For example, if a domain operator were to block the 'article19.org' domain, everything we published on it – from this report, to our coverage of the war in Ukraine, to our hate speech toolkit published 10 years ago – would become inaccessible. The DNS forms the backbone of the internet and it was not designed to evaluate or block content.

Of particular concern for ARTICLE 19 is the weaponisation of domain suspension orders by state actors to censor critical voices and prevent access to information of public interest.

Suspending a domain has an inherently high risk of blocking protected content, potentially violating international human rights standards.

Organisations such as human rights groups, journalists, and media outlets must grapple with this line of attack that threatens their ability to communicate freely online. While infrastructure-level censorship is not new,[3] the role of registries and registrars in either enabling or restricting the free flow of information requires further attention, particularly because the relationship between domain suspensions and freedom of expression is not widely understood among domain operators, civil society, or policymakers alike. To address this need, this research explains how censorship occurs at the DNS level today, and delves into the consequences of domain suspension orders on freedom of expression.

In certain situations where the DNS is being abused, such as if a domain is being used to distribute child sexual abuse material (CSAM), then domain names should be taken down to protect end users. However, how domain operators define DNS abuse – if they do so at all – varies drastically, leading to a fragmented landscape in responses to domain suspension requests. **When there is no definition at all, it becomes nearly impossible to differentiate between legitimate, warranted domain suspensions and repressive overreach that infringes upon the right to freedom of expression.** Even when DNS abuse is clearly and narrowly defined, there is still a risk that suspending the domain would be a disproportionate restriction. Furthermore, the decision whether – and how – to comply with domain suspension orders by infrastructure providers often happens **without oversight, transparency, independent review, or due process**. This is where international human rights law becomes particularly relevant in providing the necessary nuance.

All companies, including those that provide the infrastructural services and technologies powering the internet,[4] have a responsibility to respect human rights under the UN Guiding Principles on Business and Human Rights (Guiding Principles). Yet, according to our research, registries and registrars currently do not appear to honour this responsibility, including in conducting the required human rights due diligence. The lack of transparency requirements for registries and registrars has also made it harder to hold domain operators accountable. Without insight into how suspension decisions are made – let alone the outcome of these decision-making processes – there are little to no options for recourse for registrants.

Some of this is within ICANN's purview to address given its contractual relationship with domain operators. Registrars and registries must adhere to the obligations in their ICANN Contracts (Registrar Accreditation Agreement or Registry Agreement, as applicable). One of those requirements is to also follow obligations set out in the Consensus Policies. These policies are developed via ICANN's policy development process (PDP), which uses a multistakeholder model of internet governance with input from groups throughout the ICANN community.

ICANN's open policymaking processes present an opportunity to develop contractually binding commitments to human rights safeguards for domain operators. Ultimately, however, it is states who are responsible for protecting, respecting, and fulfilling international human rights law. For both state and domain operators, such contractual obligations do not preclude the need to review suspension decisions on a case-by-case basis to assess the proportionality of individual restrictions and establish accessible and robust due process mechanisms for registrants. More must also be done to build the resilience of civil society organisations at risk of being targeted by domain suspensions as tools for censorship.

This research builds on ARTICLE 19's longstanding work on the human rights implications of DNS governance issues, from engaging with ICANN to shape its policies to working with infrastructure providers to improve their internal policies.

Between June and December 2025, ARTICLE 19 conducted 23 extensive semi-structured interviews with a total of 35 representatives from:

- **11** registries,
- **4** registrars,
- **2** industry associations, and
- **6** civil society organisations.[5]

Given ICANN's central role in the domain registration industry, we supplemented expert interviews with participant observation and engagement in ICANN at four meetings between October 2024 and December 2025, as well as document analysis, including media coverage, grey literature, and relevant academic literature. This highlighted the complexity of registries' position within the broader DNS ecosystem: gTLDs are wedged between ICANN – an international body headquartered in the US – and their local or national environment. For ccTLDs, which are not contractually bound to ICANN policies, increasing regulatory scrutiny and the potential for additional regulatory burdens further complicates the situation.

This report first provides an overview of the complex and layered organisational landscape in which registries work. To explore the impact of DNS-level censorship on civil society, we highlight four cases of silencing by means of domain suspensions in **India**, **Spain**, **Nicaragua**, and **Belarus**. These examples then inform our recommendations for how to build civil society's resilience to these censorship tactics.

2

What does DNS-level censorship look like?

Case study

India: Activists' websites vanish as campaign gains traction

In July 2020, three youth organisations were in a race against the clock to campaign against a proposed update to India's Environment Impact Assessment legislation. Organisers believed that this framework for assessing development projects would endanger ecologically sensitive areas because it minimised – and sidelined – public consultations.

Combining their strengths, organisers launched an online petition in 11 languages, urging citizens to send an email in their own language to relevant government officials. Hundreds of thousands of emails were sent as the campaign gained traction. Then, the websites of the organisations sharing the petition and driving the campaign suddenly disappeared. Texts started coming in. Organisers could not access their email. The website had vanished. What was going on?

> *We changed computers, browsers. I tried using a VPN[6] [virtual private network] and it still wasn't working.*
> – Interviewee 20

Once aware that their websites were down, the impacted organisations scrambled to troubleshoot. One organisation thought it was a server issue. Another organisation checked their back end and asked individuals to access the site through different services, including via a VPN. Yet, their websites remained inaccessible. Organisations received no notice that their websites would be – or had been – blocked. It was as if their websites never existed in the first place.

Only after a deeper back end investigation of what happened did the environmental organisers discover the root cause: without warning or legal justification, the ccTLD registry operator for India had disabled their domain name. Domain names (or 'domains' for short) are like the 'directory' of the internet: without a domain, arriving at the right webpage is a nearly impossible task.

Censorship by means of infrastructure

> *Using the Domain Name System (DNS) to do content moderation, it's like using a sledgehammer when you need a screwdriver. It's the wrong instrument for the task.*
> – Interviewee 4

While infrastructure-level censorship – including at the DNS level – is not a new phenomenon,[7] growing government interest in the application of domain suspensions for censorship represents a concerning trend.[8] India is not alone in leveraging the DNS for censorship: in this report, we also cover incidents in Spain, Nicaragua, and Belarus.

The problem when trying to prevent users' access to specific online content is that suspending a domain does not actually 'delete' the content. In fact, users can still access archived content in other ways, even without a high level of technical knowledge. However, few users know how to do this. Of course, if a domain is taken down, publishers can no longer post, remove, or alter content on that domain. Moreover, users are unlikely to know that a page is inaccessible due to a domain suspension – let alone that the content is inaccessible.

Suspending a domain renders all services hosted on that domain inaccessible, including email and data storage.

This makes content moderation at the domain level particularly risky from a freedom of expression perspective because registries and registrars cannot take targeted action to remove only specific content from a webpage. This contrasts with actors 'closer to the source', who can take more targeted action against specific content. For example, a content publisher (such as a social media platform) can directly modify or remove content posted on a website, while a hosting provider can remove content from its servers (unlike a registry), thereby preventing access to it on its infrastructure.[9]

As several interviewees noted, even narrowly defined policy objectives (such as addressing copyright enforcement or online harms) often have unintended consequences without even addressing the intended goal of rendering the content completely inaccessible.[10] As an example, this could mean the suspension of the entire NYTimes domain because of one article deemed 'illegal'. This could effectively block access to all other content – from recipes to election coverage – because domain-level blocking cannot distinguish between lawful and unlawful material.

When applied to the websites of human rights organisations and media outlets, the consequences for freedom of the press, access to information, and democratic participation are severe.

Put simply, domain suspensions are at a high risk of leading to disproportionate restrictions, in violation of international human rights standards.

According to these standards, limitations on the right to freedom of expression must conform to the strict requirements of the three-part test under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). This requires that limitations must be: prescribed by law; in pursuit of a legitimate aim;[11] and necessary and proportionate in a democratic society. While the ICCPR is only binding on states (and in accordance with the Guiding Principles), there is a growing body of recommendations from international and regional human bodies that 'internet intermediaries', such as domain operators, also have a responsibility to respect human rights. For example, in a 2017 report to the UN Human Rights Council, the then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 'recognise[d] the particular impacts that infrastructure providers … have on human rights including freedom of expression, particularly in the context of surveillance and censorship'.

This means all infrastructure providers – including domain operators – must also consider the potential impact of DNS abuse mitigation actions on freedom of expression. This is especially relevant given domain registries and registrars – the entities (whether public companies, private corporations, or non-profits) that manage website addresses – face increasing pressure to censor content through domain suspensions. We will explore this in more detail in Chapter 3.

To the extent that domain registries and registrars are public companies or non-profits, the Guiding Principles would not be directly relevant. Where companies are publicly owned, they might be directly bound by the ICCPR as state actors. As for non-profits, if they are in a position to restrict freedom of expression, we believe they should also uphold principles reflected in the Guiding Principles and take steps to identify and mitigate any negative impacts for human rights, including freedom of expression.

As we see governments and private corporations turn towards digital infrastructure to censor and surveil,[12] it is important to understand both how this happens and what we can do to respond. However, to understand the full landscape of DNS-level censorship, we must first look at the broader ecosystem governing domain operators, starting with ICANN.

3

Governance of the DNS

ICANN, registry structures, and national legislation

Case study

Spain: Catalonian domains blocked in run-up to referendum

Shortly after 10:00 on 20 September 2017, the Spanish police raided the offices of the domain registry, Fundació puntCAT. The registry operates the '.cat' top-level domain, referring to the autonomous region of northeast Spain, Catalonia. The raid came ahead of a referendum to decide whether the Catalonia region should declare itself an independent country. The referendum had become extremely politically contentious, and the Spanish Government – in much-criticised action – moved to shut down any support for it.

The police confiscated all the registry's computers, arrested six members of its staff, and accused one of the company's senior executives of sedition. The police then instructed the registry to block four of its main domains, including 'referendum.cat' and 'ref1oct.cat'. The impact of the raid was instantaneous: blocking access to all webpages under those domains – including those with content that did not relate to the referendum – effectively preventing anyone from accessing information on what was undoubtedly a topic of public interest.

With little legal recourse within the country, the registry raised the alarm to ICANN to make it aware of these developments.

> *We are being requested to censor content and suppress freedom of speech in .cat domain names. This compromises the obligations we have as gTLD Registry operator towards the .cat community and may put in jeopardy our position as a steward of the Catalan speaking community on the internet.*
> – Letter to ICANN CEO

To understand why Fundació puntCAT chose to raise this issue with ICANN, we need to explain the central role of ICANN.

What does ICANN do and why does it matter?

ICANN is the multistakeholder body partly responsible for managing the DNS. Its community is structured into constituency groups that collectively negotiate policies to ensure the security and stability of the global DNS. These groups – representing the interests of end users, registries and registrars, civil society, trademark and copyright holders, law enforcement, and governments – meet at ICANN to discuss these policies.

There are two types of registries, both of which participate at ICANN: ccTLDs (those that operate country-code top-level domains, such as '.uk' for the UK, or '.br' for Brazil), and gTLDs (generic top-level domains such as '.com' or '.music'). Some registries, in turn, outsource the purchase and registration of domain names to (commercial) registrars, which effectively liaise between domain owners (registrants) and registries. While registrars sit closer to the registrant, registries set 'the rules of the road', defining the boundaries under which registrars operate. For this reason, and given more registries than registrars responded to ARTICLE 19's requests for input, this report primarily focuses on registries.

ICANN regularly gathers registries, registrars, policymakers, private sector actors, and civil society parties to develop policies that address safety and security risks. One key topic of discussion is DNS abuse mitigation.

ICANN's definition of DNS abuse

ICANN primarily works with a definition of DNS abuse, broken down into five categories. This is an influential concept because it sets the standard for when domain suspensions are 'justified' in the eyes of ICANN. The five-category definition carries weight beyond ICANN: in the regulatory and law enforcement spheres, how DNS abuse is defined determines what course of action to take in response to reported incidents of 'abuse'.

ICANN's five-category definition of DNS abuse	
1. **Botnets**	Networks of infected computers controlled remotely
2. **Malware distribution**	Spreading of malicious software
3. **Pharming**	Redirecting users to fake websites
4. **Phishing**	Tricking people into giving sensitive information
5. **Spam** *(as a means of abuse)*	Unsolicited messages used for harmful purposes

In each of these categories, malicious actors exploit the technical possibilities of the DNS. Examples include registering a fake domain to impersonate a bank in a scheme to steal customers' personal information, or registering a look-alike domain (such as articlenineteen.org instead of article19.org) that, when clicked on, infects the user's device with malware.

All operators of gTLDs (such as '.com' or '.org') are contractually bound by ICANN's definition of DNS abuse. In practice, this means that they are obligated to respond when they receive a report of abuse that is within the parameters of ICANN's definition. The response itself is up to the individual registry. However, the obligation to show that they responded is mandated in their contract with ICANN. It is this obligation that puntCAT is referring to in its letter to ICANN. But that does not mean that gTLDs cannot suspend *more* than is required by ICANN's technical definition.

Operators of ccTLDs have even more freedom to decide how broadly or narrowly to interpret reported incidents of DNS abuse since they do not contract with ICANN directly. This means that ccTLD operators are not bound by ICANN's contractual obligations, including its DNS abuse definition. Instead, these registries often maintain close bonds with national governments, whose legislation (and therefore, definition of DNS abuse) may or may not align with ICANN policies.

ICANN deliberately defines DNS abuse narrowly in an effort to limit the instances in which registries and registrars act as content moderators. Having a narrow definition for DNS abuse is one way of preventing overreach in mitigation that could infringe upon protected speech and content online. **However, this does not mean that ICANN's definition is perfect.** Moreover, it is not even universally accepted by many of the registries interviewed, which we discuss in more detail in Chapter 4.

Although an imperfect solution, having a definition – especially a narrow one, as in ICANN's case – is better than none at all.

Importantly, this definition with its narrow set of categories sets a baseline limit to the actions of gTLD registries and registrars. These categories are limited to incidents that are predominantly technical in nature and largely easily identifiable.[13] This contrasts with complaints of copyright or trademark infringement as 'abusive' behaviour via the DNS. Accusations of trademark and copyright infringement have historically been leveraged to silence human rights defenders.

Additionally, ICANN's narrow definition does not prevent registries from supplementing their terms and conditions with additional categories of DNS abuse on which they will act – and many registries have done so (see Chapter 4). Anyone – from ordinary citizens to law enforcement officials to policymakers – can file a domain suspension request. However, only when domain suspension requests map onto the five categories outlined by ICANN are gTLD registries and registrars contractually obligated to respond. Where a gTLD registry or registrar fails to fulfil these contractual obligations, a complaint can be filed with ICANN. ICANN's Contractual Compliance team will then investigate, potentially leading to the termination, temporary suspension, or public notice of breach of contract with ICANN.

Complicating this further, jurisdiction – where the domain operator is legally incorporated – matters significantly when responding to domain suspension requests. Every domain operator (registrars, plus ccTLDs and gTLDs) must comply with domestic policy within its jurisdiction. However, as discussed later in this chapter, there is currently very little legislation requiring action from domain operators.

As shown in the cases of suspensions leveraged against civil society entities outlined in this report, many domain suspension requests – including those stemming from governments and law enforcement – lack legal basis. **Yet many domain operators will still comply with requests to suspend domains even when they are not obligated to do so according to ICANN's definition or to local law.** Because suspending a domain makes all website content inaccessible, it poses a high risk of blocking access to protected and even lawful speech online, in violation of the right to freedom of expression.

Many registries do not have an easily accessible definition for DNS abuse (see Chapter 4). The ambiguity arising from attempts to narrowly define DNS abuse – as ICANN does by limiting its categories to mostly technical instances – already results in a wide variety of additional rules, mechanisms, and caveats.

When there is no definition at all, it becomes nearly impossible to differentiate between legitimate, warranted domain suspensions, and repressive overreach.

Moreover, even if a reported case of DNS abuse does align with ICANN's definition, there is still a risk that suspending the domain would be a disproportionate response.

This is where international human rights law is especially important. All infrastructure providers, including domain operators, have a responsibility to ensure their products and services are in line with international human rights law.

Domain operators must assess the proportionality of their responses to reported incidents of DNS abuse prior to taking any mitigation action – suspension or otherwise.

Yet, as we see in Chapter 5, few do so.

This also leads to a fragmented landscape for responding to these requests: a reported incident of DNS abuse at one registry may lead to a domain suspension, whereas had it been reported at another registry, the outcome would have been vastly different. The picture is even murkier when we consider the lack of transparency requirements for domain operators: registries and registrars are not required to disclose the outcome of suspension decisions or explain how the decision was made, including how they define DNS abuse in their terms and conditions.

Without this transparency, registrants and others subject to these decisions – like the environmental activists in India mentioned earlier – are left with few options for recourse or redress.

Yet, this fragmented landscape of DNS abuse definitions does not fully explain how registries determine their response to any given request. For this, we must look deeper at the registries themselves.

Registry structure

How a registry manages suspension requests that reach beyond ICANN's framework for DNS abuse depends first on whether it is a ccTLD or gTLD. Both ccTLD and gTLD registry operators are bound by national regulations; however, **gTLDs must also comply with ICANN's definition of DNS abuse**.

The registry's governance structure also significantly impacts how a registry assesses a domain suspension request, beginning with its registration model. There are generally two options: one involves the registry using a 'middleman' registrar to manage daily operations and relationship with registrants. This is the '3R model' and comprises a registry, registrar, and registrant. The other option is for the registry to manage this directly.

In the 3R model, registries delegate the commercial sale of domain name registrations to registrars. Most European and North American registries operate under the 3R model. However, Brazil, like many ccTLD operators across South and Latin America, uses direct registration instead. Rather than contracting a registrar to work with registrants, CGI.Br manages the back end operations of the domain registry, sets the terms and conditions for the '.br' domain, and communicates directly with registrants. The Colombian ccTLD registry operator is an exception in the region, with '.co' operating under the 3R model.

Whether or not a registrar is used, it is the **registry that oversees the high-level management and maintenance of domain names**. Even under the 3R model where the registrar is the first line of communication when receiving and assessing any suspension request, the registry typically implements any suspension decision. Registrars are bound to the terms set by the registry. However, according to the interviewees, the registry generally just complies with the registrar's decision on any given request.

We are therefore left with registries and registrars both trying to shift the responsibility of how to respond to suspension requests to the other, leading to ambiguity in decision-making and a lack of accountability for decisions.

Another factor is legal incorporation. Registries can operate as **non-profits**, **private enterprises** (including social enterprise companies that integrate human rights obligations into their terms and conditions), or as **independent organisations or foundations**. Many gTLDs operate as private companies. Among the registries that operate as legal non-profits, some are integrated within government ministries, while others are structurally independent but are wholly or majority-funded by the government. Many registries also operate under a multistakeholder model of governance.

A cross-section of registry structures underlines this diversity:

- **Taiwan:** TWNIC, Taiwan's ccTLD registry operator, is a non-profit that operates independently, but receives approximately 50% of its funding from the government. The government is well-represented on its board, alongside representatives from civil society and academia.

- **Colombia:** The Ministry of Information and Communication Technologies of Colombia oversees the policies and administration of the '.co' TLD. The daily management of registry services and running of '.co', including how DNS abuse is defined and mitigated, is handled by Equipo PuntoCo (a joint venture between the Team Internet Group and Colombian domain registrar CCI REG).
- **Denmark:** The ccTLD registry, Punktum dk, is a limited company that is fully owned by the association Dansk Internet Forum. The association's members and board include representatives of industry and civil society, including from the Internet Society (ISOC), an advocacy organisation committed to an open internet.
- **PIR:** Public Interest Registry (PIR) is a non-profit organisation headquartered in the US and established by the ISOC to manage the '.org' domain. Its Advisory Council provides input and recommendations on issues affecting the broader DNS community. Its Board of Directors, appointed by ISOC, oversees the registry's strategic direction.
- **Identity Digital:** Identity Digital is a private company headquartered in the US and provides domain registry services. It is owned by the private equity firm, Ethos Capital. The company either sponsors or has controlling interest in 271 TLDs.
- **Team Internet:** Team Internet is a private company headquartered in the UK that provides domain registry services. It has a corporate governance framework with a Board of Directors to manage its operations.

These diverse governance structures reflect differences in how registries define and address DNS abuse. For gTLDs, which primarily operate as private companies, profit incentives largely guide decisions on mitigation action. As opposed to gTLDs who are not obligated to do any balancing act whatsoever, many ccTLDs (and some gTLDs, notably PIR among the interviewees) would apply proportionality criteria even to 'clearcut' reported incidents of DNS abuse. But this proportionality assessment is not currently required for domain operators.

The distinct local and regional contexts in which registries operate further impacts how the registry interprets what constitutes DNS abuse in local settings. Combined with a rapidly changing regulatory landscape, this leads to vastly different outcomes for domain suspension requests.

Case study

Nicaragua: Regime 'disappears' websites of exiled media outlets

In March 2025, the regime of Daniel Ortega – the dictator in charge of Nicaragua's Government – moved to block independent websites from using the ccTLD '.ni'. Among the news sites affected were Confidencial, La Prensa, 100% Noticias, and Onda Local. According to Reporters Without Borders (RSF), more than 280 Nicaraguan media workers – including 217 journalists – have been forced into exile since 2018 as a result of systematic persecution by the Ortega–Murillo regime.[14] These four outlets continued to operate, at great risk. Confidencial is among the largest independent news platforms that still reports on Nicaragua and its entire team works in exile. According to a recent UN report, protest leaders, journalists, political leaders, academics, and human rights defenders in Nicaragua have faced arbitrary arrests, enforced disappearance, deportation, and persecution on political grounds.

When the Ortega–Murillo regime moved to suspend domains in order to silence these press organisations, the action was carried out by the National University of Engineering (UNI), the ccTLD registry operator that administers all '.ni' domains. This was to be expected; Confidencial had pre-emptively registered a different domain 'confidencial.digital' via a registry outside of the purview of UNI and Nicaraguan authorities in anticipation. However, this alternative domain would not be visible to visitors to the .ni website. In fact, site visitors had no way of knowing why they could no longer access these news outlets' websites.

The news outlets could only use social media to announce that their websites had been blocked by the government. As the news team of Confidencial posted, 'The dictatorship of Daniel Ortega has ordered the 100% Noticias site blocked under the domain .ni, in a new attempt at censorship of the independent press.' Through these posts, the registrant brought the government's infrastructural repression to light, enforcing transparency where there otherwise would be none.

However, as these news agencies were registered with the ccTLD registry operator for Nicaragua, it is out of ICANN's purview to respond. The incident instead encapsulates the power dynamics between ICANN and national governments, where domestic and regional legislation automatically supersedes ICANN policy. Moreover, the decision to suspend a domain does not (and should not) sit with ICANN. Registrants on the receiving end of domain suspension orders are therefore in a tough spot when it comes to accessing recourse. With new regulatory measures impacting DNS governance emerging, the situation is becoming even more complicated.

A shifting legal landscape

What regulatory obligations do registries and registrars have?

While most social media platforms now publish content moderation guidelines, registries and registrars have, until recently, largely escaped regulatory scrutiny. This parallel between the advent of regulatory obligations on social media platforms and the increasing regulatory scrutiny of registries and registrars is one that many interviewees observed. According to Interviewee 35, governments are also making this comparison when designing policy for 'online safety' and content moderation.

With social media companies increasingly held responsible for the content on their platforms, regulators and policymakers are asking whether registries should similarly be held accountable to 'duty of care' standards for content distributed on their domains.

Some recently adopted regulations for social media can – to varying degrees – raise certain freedom of expression risks.[15] This is now compounded with the additional risk that regulatory requirements for social media platforms are extended to domain operators, without a nuanced understanding of the risks associated with doing so at the DNS level.

Some ccTLD registry operators in Europe have secured rulings which limit their exposure to liability for the content distributed on domains they operate:

- **Sweden:** A court case involving the music pirating site, Pirate Bay, led to the ccTLD registry operator for '.se' being charged as an 'accessory to intellectual property infringement' for failing to delete the domain. Following an appeal, the court ruled that due to copyright infringement, the domain name must be forfeited to the state. Importantly, the court also recognised that the registry, in its administrative role, does not 'own' domain names. As such, the registry could not be ordered to de-register ('delete') the domain, and decisions to de-register on the basis of content would rest with the state, not the registry operating the domain.
- **Denmark:** The ccTLD registry operator for '.dk' won a case against a web host, which led to a court ruling declaring the domain registry to be 'the last resort' when addressing illegal or harmful content online. In other words, requestors – whether intellectual property lawyers, consumer protection agencies, or state actors – must first go to other intermediaries who can take more targeted action, such as a web hosting provider. Only if it is not technically possible to remove the content by other means may courts then order the registry to take mitigating action.
- **Norway:** In a 2009 ruling, the Supreme Court of Norway noted that the ccTLD registry for '.no' neither monitors website content nor has any mandate to act on websites that may appear to violate the law – that is the task for law enforcement and the justice system. The principle that the registry has no mandate to judge what is illegal content was further reinforced in 2025 when Norway's new Electronic Communications Act came into force, explicitly placing the legal responsibility for the use of a domain name with the registrant.

However, these cases might soon become the exception rather than the rule. While there are currently minimal regulatory obligations for registries, industry experts warn that this is likely to change. Given the slow pace of policymaking within ICANN, policymakers and registries have grown impatient. Without clear, actionable guidelines from ICANN on how to address very real safety and security threats exploiting the DNS,[16] governments have started stepping in with their own rules, disrupting how the global internet is governed – including in the commitment to free expression.

According to interviewees, **governments are 'discovering' the DNS system as a tool for restricting content they deem illegal or illegitimate** – and they are writing laws that allow them to use registries for this purpose.

> *We understand that in some cases, you cannot get at the actual content and the last resort is to take down the domain name, but it should be the last resort because if you do that too often, you are in essence making a lot of holes in the road and that impedes everybody's trust in the system.*
> – Interviewee 26

In the EU, the first piece of legislation to use domain 'takedowns' (a broader term that encompasses suspensions, deletions, as well as other DNS-level action) for dealing with non-compliance was the Consumer Protection Cooperation Regulation (CPC), which came into force in 2017. With the CPC, policymakers conducted an initial impact assessment to accompany the legislative proposal. Based on this assessment, policymakers justified the use of domain takedowns for enforcement of the CPC.

It has since become more common for EU policymakers to integrate a domain-deletion provision in other legislation beyond consumer protection, including for regulating online banking and the cryptocurrency market. For example, the EU's Markets in Crypto-Assets Regulation (MiCA), which entered into force in June 2023, grants competent authorities (such as financial supervisors) the power to order registries and registrars to 'delete domain names of non-compliant crypto-asset providers'. However, for reasons that are unclear, policymakers simply 'copied and pasted' this enforcement measure without conducting a prior human rights impact assessment when developing MiCA and subsequent financial legislation.

> *From there on, we saw that type of similar text as in the Consumer Protection being duplicated in the financial regulation, but it didn't include any of the safeguards.*
> – Interviewee 13

'Safeguards' in this quote refers to the initial impact assessment conducted by policymakers ahead of the CPC coming into force. This means that no justification was included in MiCA for using such a drastic enforcement measure as a domain suspension. However, even with this minimal step to assess the proportionality of using a domain suspension, the **CPC does not go far enough in safeguarding human rights**. The CPC only conducts

an impact assessment in the legislative development process; it does not explicitly require that competent authorities assess proportionality of a domain suspension in its implementation. Neither the CPC nor MiCA have an explicit requirement to assess the proportionality of using domain suspensions for individual enforcement actions. This means that less drastic alternative enforcement measures than domain suspensions were not considered.

Registries and registrars lack the technical ability to do targeted content removal, but other actors within the DNS ecosystem can. This is why using a **proportional and escalating approach** for responding to reports of DNS abuse is important. As the association representing European ccTLD registries, the Council of European National Top-Level Domain Registries (CENTR) outlined, 'intermediaries closer to the content (such as the content publisher or hosting service providers) are more equipped to address unwanted behaviour and take down unwanted content for good'.[17] Should the hosting service provider be unwilling or unable to respond to the request (such as if the scale of abusive content is widespread), only then should a higher-level actor (such as a registry or registrar) be brought in.

A proportional and escalating approach – starting with actors capable of targeted content removal – is needed to ensure safety and security considerations are balanced with the responsibility to uphold human rights safeguards.

The need for proportionality also applies in determining the appropriate response to a confirmed incident of DNS abuse. The decision to suspend or delete a domain is not a 'yes or no' answer: an escalating response procedure accounts for a sliding scale of options available for the registry. This goes beyond simply jumping to suspend a domain. Sometimes a temporary suspension is sufficient to prevent further abuse on the domain. Other times, if the registrant is uncooperative or the investigation by the domain operator shows that the scale of the DNS abuse is severe, a longer-term suspension or deletion may be warranted. Domain name deletion is a drastic measure in which the name is removed from the registry's database and becomes available for purchase by a new registrant. Alternatively, no mitigation action may be needed beyond simply reaching out to the registrant – sometimes a quick fix is all it takes. **But without using an escalating response procedure, there is a higher risk of the response being disproportionate to the reported incident**.

Both the CPC and MiCA lack transparency requirements associated with suspension decisions. Authorities simply order a suspension on the grounds of 'non-compliance' and are not required to document the decision-making process. It is a black-and-white decision to suspend or not to suspend. There is also no built-in mechanism for registries and registrars to appeal these decisions. The risk is that future regulation will continue to leverage the DNS as an enforcement mechanism without first assessing the potential consequences of such actions or providing avenues to dispute these decisions.

Domain suspensions and deletions are a blunt force instrument: even where non-compliance justifies action, infrastructure-level action can severely disrupt or impede the free flow of information. The impact goes beyond just the webpages on the domain: domain suspensions also disrupt email services. In the financial sector, suspending a bank's domain not only prevents customers from accessing their bank accounts, but it also blocks them from contacting the bank for support. In the health sector, it means not having access to medical care. In the media sector, it means being cut off from key information. This reiterates the needs for human rights accountability measures and oversight to protect freedom of expression.

Beyond the EU, national governments have also discovered domain suspensions as a new enforcement 'tool', wielding it to address other issues of national interest. The issues that are prioritised naturally vary across countries, as do the justifications:

- **Japan:** The government allows the national ccTLD operator to suspend domains on the grounds of copyright infringement. According to Interviewee 17, this is an effort by the Japanese Government to 'protect its manga and anime industry'.
- **Brazil**: The federal telecommunications regulator, ANATEL, has the power to suspend '.br' domains directly. According to Interviewee 16, this change risks expanding ANATEL's scope of work beyond its remit. The measure was part of government efforts to crack down on illegal streaming and trademark and copyright violations.
- **UK**: If passed, a proposed Crime and Policing bill, would allow investigative agencies to apply for a court order to mandate the suspension of access to internet protocol addresses and domain names associated with 'serious crime'.

However, rather than legislation that specifically addresses registries and registrars, interviewees observed it is more common to see vague and ambiguous legislation. This lack of precision leads to domain operators being 'swept in'. For example, in the EU Digital Services Act (DSA), the legislation does not explicitly designate registries as responsible for implementing the regulation. However, because registries are the only entities who can remove or disable access to domain names, they are implicated in the DSA's enforcement – albeit indirectly.

In those cases, Interviewee 25 observed that ambiguity in legislation regarding responsibility for implementation can sometimes be addressed through lobbying or better information. Ensuring regulators understand the implications of what they are asking domain operators to do helps prevent 'sweeping in' other players that probably shouldn't be involved.

Conclusion

Across all the interviews, one message kept repeating: **action by the registry and registrar must be a 'method of last resort'**.[18] This exact term came up repeatedly, especially in interviews with registries in Asia and Europe, and across registries/registrars and industry experts. All interviewees emphasised that they should never be the first actor to approach for concerns about online content. This is because any action taken by a domain operator is, by nature, inherently blunt. Registries and registrars lack the technical capability to do that 'very targeted and very surgical intervention for content', as Interviewee 13 explained. **Domain suspensions as a means of content moderation are a recipe for overreach**. For this reason, policymakers must first consider whether a domain suspension will address the issue at hand.

Registries and registrars are also concerned with liability.

Domain operators should not be arbiters of what is 'illegal' versus 'protected' online content. Only competent authorities such as regulators, courts, and state actors are responsible for content-related decisions.

Importantly, these authorities are obligated under international human rights standards to justify such decisions. Conversely, domain operators are only held to human rights responsibilities, which is a lower standard. For this reason, ARTICLE 19 is especially concerned with ambiguous legislation that risks 'sweeping in' players that are not held to the same standards.

How different entities leverage the 'blunt tool' of domain suspensions – and to what effect – is highly dependent on the affected registry's operating environment. This ranges from its relationship with ICANN and its internal governance structure to its regulatory context. This means that efforts by ICANN, policymakers, and domain operators to guarantee freedom of expression will need to be carefully tailored to the setting in which they are intended to take effect.

4

Domain suspension requests

From DNS abuse to website content abuse

Registries' definition of abuse

The request to suspend a particular domain begins with the indication that the domain owner has violated a rule: whether a law, the registry's terms of service, or principles set out by the infrastructure provider. In this chapter we provide an overview of how such violations are defined and processed by domain operators.

Registries regularly receive requests from lawyers, law enforcement, and consumer protection agencies to suspend domains. Whether or not a registry or registrar complies with the request depends on several factors, including how registries define DNS abuse. How registries define DNS abuse matters just as much as where they operate – and both affect freedom of expression.

From our interviews, we found a correlation between a registry's compliance with a given request and the extent to which that request matches the registry's definition of DNS abuse. A registry's definition, whether it sticks closely to ICANN's narrow version or lacks a clear (or publicly available) delineation completely, shapes how it responds to suspension requests. These definitions thus directly determine which content can be restricted through domain suspension.

Registries with broader or vague definitions are more likely to suspend domains, even when such actions infringe on freedom of expression.

The interviewees revealed that registries generally define DNS abuse in three different ways.

- **ICANN-aligned definition**: Limits DNS abuse to 'technical' actions that fall into the five narrow ICANN categories: botnets, malware, pharming, phishing, and spam.
- **A broader definition**: Supplements the ICANN definition by adding different types of content or online abuse that registries commit to removing under their terms and conditions, usually by suspending or deleting a domain. This addition may reflect individual preference or compliance with local or national legislation.
- **An ad hoc approach**: Registries decide on a case-by-case basis how to respond to domain suspension requests that claim DNS abuse, without clearly defining the term.

The following section explores these **three definitions of DNS abuse** and their implications for human rights.

ICANN-aligned definition limited to technical abuse

> *We try just to use a simple definition – the 'technical definition' – of DNS abuse and we try to do that as it's very simple for the registry operator to manage that way.*
> – Interviewee 35

Many registries use a definition of DNS abuse that is nearly (or completely) identical to ICANN's definition of DNS abuse. This means that DNS abuse encompasses a limited number of narrowly-defined activities that fit neatly within the categories of botnets, malware, pharming, phishing, and spam. The ICANN definition functions as a kind of minimum standard in the registry space. Of the 11 registries included in this report, 4 directly quoted ICANN's definition for DNS abuse in their terms and conditions.

The centrality of the ICANN definition varies, however, across registries. All gTLDs will have this minimum standard in their terms and conditions, because their ability to operate TLDs (.biz, .org, .com) rests on its contract with ICANN (see Chapter 2). It is also a popular reference point for ccTLDs, the operators of national domain spaces. For example, NIC Chile cites ICANN's definition of DNS abuse verbatim when assessing applications to register a '.cl' domain name. While ccTLDs have even more flexibility than gTLDs, it is common for both gTLDs and ccTLDs to add additional categories of actions that can trigger a domain suspension or prevent domain registration.

For example, the ccTLD operator for '.co' in Colombia defines DNS abuse in exactly the same terms as ICANN; however, its anti-abuse policy includes a clause allowing the registry at its sole discretion to 'expand the scope of this policy to include other forms of online harm, such as impersonation attacks, CSAM, fraudulent activities, and violations of applicable law'. As seen here, the registry operator can broaden the definition of DNS abuse to encompass a much wider range of issues than the five categories set out by ICANN.

Another example that goes further than Colombia is Ireland. The terms of service for Ireland's ccTLD operator for '.ie' includes a clause allowing the registry to 'cancel or revoke, alter, or amend a domain name registration … where the domain name is defamatory, racist or contrary to public policy'. Whereas ICANN policy just calls for DNS operators to 'take action' on DNS abuse, Ireland's ccTLD operator goes further by listing 'what' the registry can do to respond.

The ccTLD operator for India's '.in' is even broader in its DNS abuse mitigation policy, noting that 'in exceptional cases recognized as seriously abusive' the registry may initiate 'appropriate action' on the following categories: 'child sexual abuse materials, controlled substances (content in relation to sale or trade of prohibited or illegal goods), human trafficking, violent extremist content, and hate speech'. Its DNS abuse policy not only covers a much broader range of activities but also uses more ambiguous terminology (such as 'universally recognized') that leaves ample room for interpretation.

Typically, these additional actions will not be designated as DNS abuse. Rather they will be listed as actions that are 'abusing the domain' by violating either the law and/or the registry's terms and conditions, which will, nonetheless, result in a domain suspension.

Broader definition of technical abuse including limited content or online abuse

> *We're not here to censor all content online and particularly commercial harms. We don't get into that. Actual threats to human safety and wellbeing … things like imminent threats to specific humans, those are the kinds of categories that we will act on.*
> – Interviewee 34

The ICANN definition of DNS abuse is meant to help domain operators distinguish between incidents that meet the threshold for requiring registry action versus those that are outside its purview. Theoretically, anything beyond the five categories defined by ICANN (for gTLDs) or the registry's terms and conditions (for both ccTLDs and gTLDs) would require an order from a court or other relevant authority to prompt the registry to act.

However, in practice, many registries have identified specific instances where the registry can respond with a suspension *without the need for a court order or warrant*. In their terms and conditions, these registries may distinguish between 'technical abuse' and other kinds of suspension-worthy abuse. Registries utilise a variety of terms for these kinds of DNS abuse, including 'content abuse' and 'online abuse'.

Some examples include:

- **Australia:** Australia's ccTLD registry operator, auDA, has a country-specific process for managing trademark and copyright disputes called 'auDRP'. Copyright infringement, however, is not designated as 'illegal content'.

- **Denmark:** Denmark's ccTLD expands the ICANN definition of DNS abuse by adding 'issues of security or public interest' as grounds for suspending a domain name. To do so, two conditions must be met: 'the domain is used in connection with manifestly illegal acts or omissions that infringe substantial considerations of security or public interest' and 'the circumstances call for not awaiting a decision from the Complaints Board for Domain Names or the courts'.
- **gTLD for '.asia'**: DotAsia supplements the ICANN definition with two additional categories of technical abuse. It also adds a category of content-related abuse: 'distribution of child pornography' will trigger a domain suspension.
- **gTLD for '.org':** PIR distinguishes between 'DNS abuse', which it defines in alignment with ICANN's definition, and 'website content abuse'. Interviewee 34 stated that 'anything related to content is not DNS abuse' as, in PIR's view, 'DNS abuse' is a purely technical term. However, PIR will comply with limited requests to suspend domains for non-technical abuses in specific use cases outlined in its terms and conditions.

There are also overarching efforts to designate a limited set of non-technical actions as 'abuse of the DNS' that require suspension across registries and registrars. For example, signatories to the Framework to Address Abuse have agreed to four categories of 'web content abuse' on which the registry or registrar can take action without awaiting a court order: 'the distributions of child sexual abuse materials; the illegal distribution of opioids online; human trafficking; and specific and credible incitements to violence'. Whether the registry informs authorities of this response depends on the individual registry's jurisdiction (for example, domestic legislation may require a registry to notify authorities and/or impacted registrants) and its terms and conditions.

Importantly for this broader DNS abuse definition, registries have tried to clearly distinguish between 'technical' abuse – as aligned with ICANN's definition – and anything content-related, which can range in terms of the specific 'content' but is largely limited to what tends to be illegal under domestic law.

No clear definition of DNS abuse

All registries interviewed shared insights into how they typically respond to requests for domain suspensions, including detailed procedures and communication processes. However, not all had an easily accessible definition for DNS abuse, with a murkier picture for ccTLD registries.

For ccTLD registries, a lack of a definition in their terms and conditions leaves ample leeway to decide how to respond to a domain suspension request that pertains to content. As they are not contractually bound to ICANN's definition, some ccTLD registries do not bother to define DNS abuse at all.

The grey area that comes up when trying to define DNS abuse in specific technical terms, as ICANN does, already leads to a great variety of additional rules, mechanisms, and caveats. **If neither the ccTLD registry's terms and conditions nor local legislation provide any guidance, it is up to the registry's discretion how to respond.**

For some ccTLD registries, if the law does not provide a clear answer, the registry will err on the side of caution and not suspend. According to Interviewee 13, this is the case for most EU-based registries: when requests come from intellectual property lawyers, police officers (without a warrant or court order), or the general public, the registry will not suspend. Instead, it will decide how to respond on the basis of the nature of the request (for example, what the request is about) and the requestor (is it a random person versus a law enforcement official with legal grounding). However, for others, the simplest thing for the registry to do is to either completely ignore or simply comply with the request.

Moreover, when there is no definition at all, it becomes nearly impossible for stakeholders (including authorities and impacted entities) to differentiate between legitimate, warranted domain suspensions, and repressive overreach.

Without transparency requirements, it is left to the discretion of registries and registrars to disclose how a suspension decision was made and upon what grounds. Without this information, it becomes nearly impossible for registrants to contest a domain suspension decision. This is where the threat to freedom of expression is highest.

> *We have a longstanding policy that we don't look at content. We are not the police. We can't decide if something is illegal or not.*
> – Interviewee 11

Without the constraint of a definition, ccTLD registries make ad hoc decisions about how to respond to a domain suspension or blocking request. This poses significant problems for those making the requests (such as law enforcement officials, judges, intellectual property lawyers, child rights advocates) because their effectiveness depends on them correctly understanding what kinds of requests fall within the registry's purview.

However, ad hoc or haphazard decision-making in relation to domain suspension requests is not just rooted in a lack of clear definitions. Nearly all registries interviewed maintained a 'loophole' in their terms and conditions. This loophole allows the registry to suspend a domain at their own discretion, including for reasons beyond what could be considered abuse – technical, online, or otherwise. The loophole, even if never used, effectively gives registries the power to arbitrate speech on all the domains they oversee.

This raises the question of who watches the watchmen – which brings us back to ICANN.

ICANN and DNS abuse mitigation: Risks and opportunities

> *Right now, within ICANN, there's no due process obligation for any registry or registrar that suspends a domain name for DNS abuse … There is nothing in our contracts that requires a registry or registrar to have any sort of contact where a registrant can say 'I think you got this wrong'.*
> – Interviewee 34

ICANN generally does not concern itself with how registries and registrars expand DNS abuse categories in their terms and conditions. As long as gTLDs registries and registrars comply with the baseline definition of DNS abuse, ICANN refrains from commenting on the power domain operators assume for themselves in these documents. ICANN is not a regulatory body and strives to remain apolitical; however, its decisions – or the lack thereof – have far-reaching implications.

Even with the categories covered by ICANN's definition, there is a perception among members of the Government Advisory Committee (GAC)[19] – representatives of national governments at ICANN – that contracted parties (gTLD registries and registrars) are not doing enough to counter DNS abuse (both according to ICANN's definition and beyond). According to several

interviewees, GAC members are frustrated by the current rate of mitigation efforts, which they see as far too slow relative to the reported rise of DNS abuse incidents. Governments have sought to reassure their citizens that work is being done to prevent DNS abuse, particularly when it comes to phishing and spam via the DNS. Until recently, government representatives at ICANN had been willing to play by ICANN's rules and patiently await the completion of ICANN's policymaking processes to address DNS abuse. But this is changing. In the EU, as discussed earlier (see Chapter 3), there is already legislation integrating domain-deletion provisions.

ICANN has repeatedly emphasised that 'ICANN does not take down domain names – we have no technical or legal authority to do that. We have no involvement in the takedown of any website, which is an issue of national authority.' According to its bylaws, ICANN also will not regulate the content carried or distributed by the DNS. **This essentially means ICANN must remain content-neutral in its policymaking.** Moreover, ICANN has no jurisdiction over the operations of ccTLD registries. However, this does not mean that ICANN is unable to do anything.

Striking the right balance between the interests of stakeholder groups with disparate (and often, competing) views on how to address DNS abuse is paramount. This is where ICANN comes in.

While an imperfect forum, ICANN's multistakeholder model of governance presents a starting point for how to integrate a diverse set of inputs into governance of the DNS. There is space – and arguably, a need – for ICANN to show its capacity to 'meet the moment' by successfully developing DNS abuse mitigation policy. Having a narrow definition of DNS abuse is a good starting point, but there is more that ICANN can do to uphold human rights safeguards via its contractual agreements. This is something for which the non-commercial stakeholder group (NCSG) has long been advocating with the view of establishing rights-respecting DNS abuse mitigation policy. Its open policymaking process provides opportunities to integrate human rights safeguards into ICANN's Consensus Policies, which are binding on contracted parties (gTLD registries and registrars).[20] Changes to ICANN obligations can, in turn, influence the operators of ccTLDs to protect freedom of expression. When a policymaking process leads to a Consensus Policy, contracted parties are contractually obligated by ICANN Contractual Compliance to adhere to the policy requirement. **In this way, ICANN contracts and Consensus Policies can serve as a tool to uphold human rights.**

Under the Guiding Principles, companies – including domain operators – have a responsibility to respect human rights, independent of state obligations or the implementation of these obligations. This includes conducting due diligence and human rights impact assessments to identify, prevent, and mitigate any potential negative human rights impacts of their operations, and incorporating human rights safeguards by design to mitigate adverse impacts.

Despite this, few registries or registrars have integrated such safeguards into their DNS abuse mitigation procedures.

For example, an outcome of a policymaking process could be a Consensus Policy requirement that contracted parties offer recourse mechanisms for registrants, such as the provision of pathways to contest suspension decisions. In this case, if the Nicaraguan news organisation 100% Noticias had been registered with a gTLD registry, that registry would have been required to demonstrate that it has a mechanism for accepting complaints and that it properly reviewed the complaint submitted by 100% Noticias. If the registry failed to comply, then the registrant could notify ICANN Contractual Compliance and the registry could potentially face legal consequences.

Integrating human rights safeguards into ICANN's contracts with gTLDs and registrars is a powerful way for ICANN to support registrants' rights.

Arbitrary or inconsistent suspension of domains, especially without legitimate reasoning and without due process (such as registrants' ability to contest suspension decisions), poses a threat to the security and stability of the DNS. Through changes to its contractual agreements with gTLD registries and registrars, ICANN can – and should – hold the domain operators with which it contracts accountable for the potential (mis)use of 'abuse' in their terms and conditions and in their domain suspensions.

Conclusion

Registries define and respond to DNS abuse in a variety of ways. While ICANN provides a definition with which all gTLDs and registrars must comply, this merely sets the baseline. Registries are free to build upon this definition by adding additional categories. ccTLDs have even greater freedom to define DNS abuse, as they are not contractually bound to ICANN's definition. Both ccTLDs and gTLDs must navigate national priorities, political interests, and an evolving

regulatory landscape. There is, therefore, a clear incentive for registries to supplement the ICANN definition with DNS abuse categories that reflect local norms and priorities, even when those might be at odds with international human rights standards.

Since there is no consistent definition of 'abuse' across domain operators, suspension requests on the same grounds might succeed at one registry but be rejected at another. Further complicating this definitional dynamic is the fact that new regulations often lack clear definitions (as exemplified by the Digital Service Act, discussed in Chapter 3). This ambiguity means registries may be called by regulators to act 'by default'. As the only entities technically capable of doing so, registries and registrars are requested to comply with legislation to 'delete' or 'suspend' a domain, even if they are not mentioned directly in legislation. As a result, even registries that hold to a narrow, technical definition of DNS abuse may find that legislative changes supersede their terms and conditions.

This is why integrating human rights safeguards into legislation is even more important. States have the ultimate responsibility to uphold international human rights law. In relation to domain suspension orders, governments can and should provide accountability mechanisms, such as access to recourse and redress mechanisms for registrants whose domains have been unfairly suspended. Transparency requirements that clarify domain operators' decision-making processes and the outcomes of those processes are also integral for registrants to appeal such decisions.

Yet even without external regulatory pressure, the breadth of definitions for DNS abuse in the registry space poses a risk to freedom of expression. The range of definitions in registry terms and conditions gives the registry a lot of leeway to independently decide if and how they respond to requests for domain suspensions or blocks. This creates a tricky balancing act for registries and registrars, who must decide for themselves how to navigate these tensions.

As the next chapter lays out, what registries and registrars prioritise varies enormously in practice.

5

Procedural differences

When and how to respond to reports of DNS abuse

Once a registry or registrar has determined that a domain suspension request is valid and one of its domains violates either the registry's terms and conditions or local laws, it must decide how to respond. Interviewees shared their registry's processes and procedures for handling DNS abuse.

While procedures and outcomes differ across registries, three determining factors remain constant when registries and registrars decide how to respond to a request:

1. Who issued the request?
2. Did the request originate in their jurisdiction?
3. What do their terms and conditions stipulate?

Who issued the request?

Requests for a domain suspension typically come from one of four entities:

1. Law enforcement,
2. Intellectual property lawyers,
3. Judicial system, or
4. Consumer protection or watchdog agency

Registries will weigh the position of the entity issuing the request when they decide whether or not to respond to a domain suspension request.

Law enforcement

According to interviewees, law enforcement agencies are turning to domain operators to leap directly to the 'source'. In that process, registries often come to the forefront as a suitable or even 'natural' place to try to address anything deemed illegal. As Interviewee 13 observed, domain takedowns are a 'lucrative tool' because 'it's easier to go to the source on the infrastructure level rather than trying to address it with numerous actors that are within the content supply chain'. Law enforcement agencies can lighten their workload by turning to registries first.

Law enforcement agencies are also interested in registries because registrant information (such as their address, phone number, when they registered the domain) can serve as additional evidence or clues for their work. From this perspective, suspending a domain is a quick and effective way to prevent and stop fraud and other cybercrime, such as phishing and malware distribution.

These suspension requests are a tricky area for registries and registrars. Law enforcement agencies, particularly small, local agencies, often lack the technical knowledge necessary to understand how domain operators work. This means that they often do not adequately understand what registries and registrars can or cannot do. Interviewees noted with frustration how often they receive requests that are out of their technical purview (such as requests to block URLs, which registries and registrars cannot do). Interviewees also noted that they will often receive requests asking them to respond disproportionately (such as suspending an entire domain just because there was one webpage with objectionable content). For some registries, such requests are in violation of their terms and conditions or incompatible with their mission.[21]

The ambiguity between ICANN's contractual obligations, an individual registry's terms and conditions, and the regulatory burdens imposed on registries by its jurisdiction leaves clear governance gaps when it comes to DNS abuse mitigation. For these reasons, it can be challenging for registries to decide how to respond: resisting such requests could lead to lengthy disputes (and is not always an option if mandated by law), while simply complying carries the risk of taking down protected content.

Intellectual property and trademark infringement lawyers

It is extremely common for registries and registrars to receive suspension requests that reference copyright. The requestors typically turn to registries because taking down a domain is a quick and 'efficient' way to prevent the dissemination of content. It is also faster than other pathways. Where the rightsholder or relevant lawyer would otherwise need to find and contact the web hosting provider for each webpage that features the content, turning to the registry means that they can take down several webpages at once. Registries typically respond to these requests by pointing requestors to ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) for trademark-based domain name disputes and taking action in accordance with that policy. Some ccTLD registries have their own domestic version of the UDRP, which functions similarly.

Many registries interviewed noted that judging whether a domain is in violation of trademark or copyright law is outside their purview, but that they will respond in line with the ICANN framework or with court orders. However, this line is more difficult to maintain for registries that do include content-related abuse in their terms and conditions. This allows requestors to argue that trademark infringement is a type of 'content abuse' and – even if it is not in line with the ICANN definition of the term – should lead to a suspension.

In other words, the concept of 'content abuse as a form of DNS abuse' creates wiggle room that requestors can leverage to argue that their interests (such as copyright or trademark infringement) also apply.

Requests that bring trademark and intellectual property concerns as matters of DNS abuse are already being used to silence online speech. Interviewees noted that law firms will pressure registrars to suspend the domains of independent media organisations after claiming copyright infringement. ARTICLE 19 Mexico has extensively documented how copyright law is already being used by governments to take down content as part of a broader effort to stifle dissent and press freedom in the country. As seen in Spain (Chapter 3, case study), the impact of this tactic when applied at the infrastructure level has resulted in the curtailment of free speech and the exercise of democratic rights.

Court orders

These requests are usually uncomplicated from the point of view of registries and registrars. Domain operators are not (and should not be) arbiters of what is 'illegal' versus 'protected' online content. As the former Special Rapporteur on freedom of expression noted in his 2016 report to the UN Human Rights Council, 'private intermediaries are typically ill-equipped to make determinations of content illegality'. Only competent authorities (such as regulators and the courts) are responsible for content-related decisions. Both ccTLDs and gTLDs must therefore comply with a suspension order from a judge or a regulator in their jurisdiction.

However, registries (both ccTLDs and gTLDs) and registrars also currently lack pathways to further clarify or contest suspension orders from the courts. This has led to situations where domain operators are legally obligated to comply with overly broad requests with few (or no) avenues for recourse. This is because there are few recourse mechanisms available for registries themselves to contest suspension orders from courts or national governments in their jurisdiction. But that does not mean registries should do nothing.

Domain operators have a responsibility to 'engage in prevention and mitigation strategies that respect principles of internationally recognised human rights to the greatest extent possible when faced with conflicting local law requirements'.[22] Options include soliciting assistance from civil society, other government authorities, international and regional bodies, and other stakeholders to explore all legal options for challenge. Some interviewees highlighted that they have appealed such orders when they disagreed or saw them as overreach. Whether such pushback is possible usually depends on the

size of the registry and its jurisdiction. Larger organisations have the means to hire lawyers to carry out these appeals, which can be lengthy, whereas smaller ones do not.

Despite these options, registries are still very limited in their ability to dispute domain suspension orders coming from state actors. This is where the registry's jurisdiction becomes even more salient.

Consumer protection or watchdog agency

Organisations focused on child safety online, among other consumer protection and watchdog agencies, also issue requests to registries and registrars to suspend domains. It is generally up to the domain operator's discretion how to respond to such requests. In some jurisdictions, court decisions or regulation may obligate the domain operator to comply with a suspension order when it relates to a specific issue (such as CSAM). Some registries in their terms and conditions designate specific consumer protection organisations, such as those preventing the dissemination of CSAM, as 'trusted notifiers'. When a registry receives a request from a 'trusted notifier,' it will take immediate action.

Registry's jurisdiction

A second factor in how registries respond to suspension requests is jurisdiction: where the registry operates and where the request originates. Although registries are often only legally required to comply with requests from their own jurisdiction, suspension requests can also come from other jurisdictions. How registries handle this friction between global infrastructure and national law directly impacts freedom of expression: their decisions determine what information is available to whom, and where.

The local character of legal systems and the global nature of the DNS put registries in a position where they must decide whether and how to respond to requests that come from other jurisdictions. Governments will sometimes cite domestic legislation to explain why they ordered a domain suspension. In the case of the Indian environmental activists, the government did not make any attempt to justify its actions, declining to acknowledge that the suspension had even taken place.

How a registry responds to a request is truly a matter of discretion. Even if the request comes from law enforcement or a court, the **registry is only legally required to comply with the request if it originates in the jurisdiction in which the registry operates**. One effect of this is that organisations that register their domains with a ccTLD to post sensitive content about their country's

(repressive) government often must move to a gTLD registry outside of their region over the long term. This is because organisations based in jurisdictions without strong democratic processes could risk retribution should they try to contest such suspension orders.

The close connections between country-code domain operators and governments make using a ccTLD registry too risky for most organisations engaged in politically sensitive work. All organisations discussed in this report ultimately moved their domains to gTLD registry operators based in the US, a country traditionally known for its liberal freedom of expression laws. They assume, correctly thus far, that registries headquartered in the US are unlikely to comply with suspension requests from a foreign government.

Nearly all registries interviewed reiterated that they did not want to act as private judges and preferred not to decide whether an action was illegal. But as several interviewees emphasised, **the registry does not have to comply with every request it receives**. If the request is about content that complies with local law and is not accompanied by a court order, the registry can refuse to comply with it. Specifically, when a request originates from outside a registry's jurisdiction and aligns with neither ICANN's definition of DNS abuse nor their own terms and conditions, registries can often choose not to act on it.

In this sense, a registry's decision to act will be solely based on its terms and conditions, which is where the highly differentiated definitions of DNS abuse(s) that the registry has committed itself to act on become acutely relevant.

Registry/registrar terms and conditions

The individual registry/registrar's terms and conditions play a critical role in the response to requests to suspend a domain. For example, PIR, the gTLD operator for .org, is based in the US. If a court from outside the US orders PIR to suspend a domain that is being used to disseminate CSAM, that court order is not directly enforceable against the registry. **However, PIR might decide to comply with the requested action because CSAM is one example of 'online content' abuse according to PIR's terms and conditions.**

The terms and conditions also reveal and reflect the organisational structure of the registry or registrar. For many registries, the terms and conditions stipulate who within the entity has the authority to make the final decision on whether to comply with a suspension request.[23] For example, the terms and conditions for one of the registries interviewed specifies that the board member who is a representative of the country's ISOC chapter has the final say on domain suspension requests. Some registries delegate the decision-making process for domain suspension to an external expert (such as a watchdog organisation

or trusted notifier) for specific instances, such as for reports of CSAM. In this sense, the terms and conditions directly connect the operating environment of the registry – its institutional location and internal structure – to its decisions about content. This also showcases how terms and conditions are incredibly fragile documents, capable of being wielded to suppress free expression.

To contact or not to contact the registrant?

Registries and registrars face a complex and multifaceted calculation whenever they consider what action to take when responding to a request to suspend a domain. Once a decision is reached, determining the role of the registrant is no less complicated.

The process for communicating with the registrant is a function of the registration model. Registries that operate without the middle layer of a registrar will usually communicate with the registrant directly. For registries operating under the '3R model' (where the registry contracts a registrar to manage customer relations with registrants), the registrar is closest to the registrant. This means that any suspension requests will usually be referred to the relevant registrar. If the registrar, upon completing its investigation, decides that the right course of action is to suspend the domain, it will forward this request to the registry to implement. In this model, the registry only becomes involved in the decision in case of an escalation, such as if the registrant disagrees with the registrar's decision. Whether to inform a registrant of the decision to suspend is therefore up to the registrar.

Registries also vary in whether and how they publicise suspensions afterwards. According to Interviewee 16, the Brazilian Government maintains an ongoing list of domains that have been suspended, but **this list is not publicly available, and registrants are not informed that their domain is on this list.** In practice, this means registrants will need to independently confirm that a domain suspension is the reason why their website is inaccessible. Only then can registrants begin to appeal the decision. This example underlines the importance of transparency and accountability measures when it comes to domain suspensions. Transparency is crucial for registrants' ability to appeal suspension decisions if they believe the decision violated their free expression online.

Conclusion

From the perspective of a registry, only one type of suspension request is relatively simple: court orders from a registry's own jurisdiction. Even in those cases, a court order to suspend a domain can still violate international human rights protections for freedom of expression. For all other types of suspension requests, registries must make judgement calls based on their definition of DNS abuse, their terms and conditions, and local law.

Because the circumstances vary so dramatically across registries, requests made on the same grounds might succeed in one place but be rejected in another. This fragmentation leaves registrants facing unpredictable, often arbitrary decisions with little transparency and even less recourse.

While there is much out of their realm of control, registries *do* have the power to change their internal policies and how they communicate externally. The next chapter provides positive examples of how registries and registrars are integrating appeals and recourse mechanisms for registrants impacted by DNS abuse mitigation action and explores how both domain operators and states can go further to uphold international human rights responsibilities and law.

6

Due process and accountability for resilience

Case study

Belarus: Journalists' association censored beyond borders

In 2023, the ccTLD registry operator for Belarus requested documents from the registrant for 'baj.by', the domain representing the Belarusian Association of Journalists (BAJ). The request specifically ordered that the documents be presented in person as part of a mandatory 'identity verification procedure'. A registry requesting in-person identity verification is strange enough. Stranger still, there was nothing in the registry's terms and conditions at the time requiring the registrant to come in for verification (this requirement was only added *after* the registry issued the request to BAJ). With the registrant unable to comply at the risk of their personal safety, the registry suspended the domain.

Though BAJ has existed for over 30 years, it has been operating in exile since 2021. Interviewee 31 said that it is a common tactic in Belarus for the government to claim human rights organisations are in violation of 'anti-extremism' legislation as a means of repression. BAJ's website had already been targeted by the government for allegedly 'hosting extremism materials'. By targeting BAJ's domain, the government leveraged its power over the Belarusian ccTLD registry to repress speech beyond its borders. The consequences of the suspension decision were compounded by the lack of transparency on the part of the registry. The registry not only neglected to notify BAJ of the changes to its terms and conditions that led the registrant to be considered in 'breach of contract,' but it also did not offer any reasonable pathway for BAJ to restore access to its domain.

The domain suspension itself was just the start: when BAJ's domain was suspended, the organisation had to find and register a new domain. This required significant resources and time to migrate all the news outlet's web pages, and to create new email addresses for all staff. BAJ then had to inform its entire network of these changes to ensure their safety. Sources who were contacted by an email address connected to BAJ's old domain were at risk, because they could unknowingly be speaking with government officials. Sharing sensitive or confidential information with a government informant would endanger themselves and others.

Transparency, in this sense, is a way to preserve the safety of end users in the face of repressive regimes.

What more can registries do to protect registrants?

This chapter examines what happens after a domain is suspended. Or, more accurately, what *should* happen, but rarely does. We map the current state of redress and accountability in the domain space, from due process mechanisms to transparency reporting and appeals procedures. Most registries lack these safeguards entirely, meaning registrants often don't know their domains were suspended, why it happened, or how to contest the decision. We then highlight emerging practices from registries beginning to build accountability into their operations, offering models for how the domain industry can better protect freedom of expression.

In the context of registries, respect for human rights includes providing those impacted by domain suspensions with opportunities to challenge the decision. Yet, this is rarely the case as things stand.

The stakes are clear: without appeal or redress mechanisms, domain suspension becomes an unchecked tool for censorship, leaving registrants with no recourse or path to remedy.

Registries also face conflicting demands from all sides: requests from courts and law enforcement or domestic legal obligations that may conflict with human rights responsibilities; their own DNS abuse policies; and their contractual obligation with ICANN. ICANN's narrow definition, varying registry definitions, and complex regulations, leads to widely disparate outcomes for suspension requests made upon the same grounds.

These conflicting demands and requirements are not only a challenge for registries but also expose registrants to human rights risks. In cases of alleged violations, registrants must be able to challenge the registry's actions.

However, most registries lack accountability mechanisms, and many also fail to provide even basic transparency.

This is not simply ARTICLE 19's observation, but an often-repeated fact amongst the registry community. As one of them stated:

> *A lot of the remedies available under human rights law [such as appeal/dispute mechanisms] are limited to those who are directly affected. So, if none of those people know, or are in a position to challenge the deprivation of their*

> *rights just because they don't know what's happening … you're short-circuiting any type of human rights remedy.*
> – Interviewee 22

Traditional human rights instruments require evidence of DNS abuse to access a potential remedy. The problem is that registrants often don't even realise their domains have been suspended, let alone have a path to challenge the decision. Without this information, it becomes nearly impossible to dispute or appeal any suspension decision.

Building mechanisms to allow registrants to see and understand registries' procedures for decision-making is a way to hold registries accountable for the impact of their decisions. It also builds resilience against restrictions to freedom of expression via domain suspensions.

The next section provides examples of how registries and registrars are beginning to integrate accountability and due process mechanisms into their operations. It also emphasises the importance of developing accessible dispute and appeals mechanisms for when things go wrong.

Respect for human rights: Due process, transparency, and appeals

Registrants' access to remedy and procedures for transparency varies widely across registries. The majority of registries and registrars interviewed expressed interest in what accountability could look like in the domain operator space, but such practices are currently not industry standard. They also demonstrated that accountability is a fluid concept.

> *People always want registries and registrars to quote, 'do more' and quote 'be more responsible'. But being responsible in this space doesn't mean just suspending everything in sight. Being responsible means having processes in place in case you get it wrong.*
> – Interviewee 34

When asked why accountability remains an afterthought, some interviewees noted that the concept may not be widely understood as part of a registry's work. Infrastructure providers, both within and outside the domain space, have long operated invisibly, without significant regulatory burdens or societal scrutiny.

To integrate due diligence and accountability procedures in the technical work of domain management would also acknowledge that domain operators make decisions about content, and that these decisions have human rights implications – in other words, that **their technical work is political.** This could lead to additional oversight, increased regulatory obligations, or greater pressure to use their infrastructures to restrict freedom of expression. One interviewee speculated that the reason some registries – particularly larger ones offering more services than just DNS management – may not want to integrate transparency and accountability requirements is due to concerns about adding complexity to their operations. From attending ICANN meetings, we observed that some operators view integrating such procedures as technically burdensome and unnecessarily complicating their core work.

Still, efforts towards accountability are underway. PIR, the gTLD that operates '.org', has developed a set of Anti-Abuse Principles outlining the registry's duties towards registrants. This includes PIR's commitment to a publicly available appeals process and its responsibility to act on reports of DNS abuse, which are balanced against the threat of censoring legal and legitimate speech. Australia's ccTLD registry operator, auDA, similarly launched a multi-step compliance procedure that is anchored in a set of core principles and commitments. The document includes the registry's intent to help registrants access complaint procedures and guide them in appealing decisions before suspending a domain. Other domain operators are also beginning to integrate due diligence and accountability measures in their services. Cloudflare, for example, has a specific section of its website dedicated to due process across its services, including a detailed explanation on its approach to law enforcement requests. Importantly, these accountability and due process procedures are all easily accessible on its website. These are all promising developments.

What does transparency look like for registries and registrars?

> *We cannot stay behind and say we only have the technical infrastructure we are responsible for … [and] we don't have anything to do with content. We have to make sure that there is a balance.*
> – Interviewee 19

Once the decision to suspend a domain has been made, the registry or registrar must decide if and how to communicate this decision. Depending on the domain operator, the registrant may not be informed that their domain has been suspended – as in the case of the Nicaraguan journalists. In those cases, users trying to access the website will simply see an error message.

The error message is unfortunately the norm when a domain suspension request is behind a website's inaccessibility. However, there is an easy solution here for registries wanting to be transparent and communicate to site visitors that they are looking at the outcome of a domain suspension order: **set up a landing page**.[24] This means creating a special webpage for the websites on a domain that has been suspended. When end users try to access the website, instead of seeing the original webpage, they are redirected to an alternative webpage that has an explanation for why the website is inaccessible. The landing page can also note whether the suspension was implemented upon government request, and even the specifics of the legal basis (distribution of CSAM, sale of fraudulent or illegal goods, etc.).

While still very limited in the domain space, transparency reporting towards the public is becoming more common. In the domain space, Cloudflare publishes the actions it has taken in response to reports of DNS abuse and legal orders. Its abuse processes report presents data categorised into actions the registrar has taken on content distributed by domains it manages, mitigation action on phishing and technical DNS abuse, and suspensions of services (broken into further categories of US court orders, copyright/trademark dispute resolutions, termination of services due to CSAM, and voluntary terminations).

Similarly, both auDA and PIR regularly publish statistics on the number and types of suspension requests they receive. For auDA, this is in the Compliance section in its quarterly report, broken down into categories. PIR's Anti-Abuse Metrics provides granular detail, with sections on the number of suspensions for DNS abuse and court-ordered actions on domains. Data is sorted by type of DNS abuse and includes court-ordered civil intellectual property enforcement, as well as each of the 'limited categories of website content abuse' detailed in its terms and conditions.

These efforts are critical because they contribute to a public that is informed about the mechanisms and procedures that govern online speech. Especially in infrastructure contexts, these processes often remain invisible, and this lack of visibility alone can threaten freedom of expression. For this reason, more work must be done to ensure that these procedures for transparency and accountability become standard, rather than exceptional. Domain operators can also learn from transparency requirements for social media platforms.

Conclusion

BAJ's experience exemplifies the far-reaching consequences of domain suspensions and highlights the importance of accountability mechanisms, as well as the urgent need for governments to take action to protect registrants.

Stakeholders must carefully consider whether a domain suspension – or any action at the DNS level – is the appropriate response to the issue at hand. As highlighted in this chapter, registrants have little recourse to appeal or contest suspension decisions. Moreover, they are not even usually informed that their domain is the target of a suspension decision. As ARTICLE 19 has repeatedly emphasised, detailed reporting of DNS abuse mitigation action and the establishment of complaint and appeals mechanisms are crucial steps domain operators can take towards fulfilling their responsibility to uphold human rights.

Yet even with the best intentions, mistakes can still be made. This is where ICANN has an particularly important role to play. The ICANN policymaking process provides a clear avenue to establish human rights safeguards for DNS abuse mitigation that are contractually binding. Moreover, the potential human rights impact must be considered at each step of the policy development process (PDP). Here, the priority should be on developing accessible, standardised recourse mechanisms for registrants impacted by DNS abuse-related mitigation actions.[25] Examples include establishing pathways for registrants to appeal suspension decisions (and, where applicable, have their domains restored), clear and fair processes through which registrants can file complaints or appeal mitigation actions, and developing transparency requirements for DNS abuse-related actions.

While these mechanisms would represent a positive step forward, there are clear limitations to what registries alone can do. Given their responsibility to uphold international human rights standards, governments must lead the charge in establishing recourse mechanisms for domain operators to appeal suspension orders. States should not subject internet intermediaries to mandatory orders to remove or otherwise restrict content, except where the content is lawfully restricted in accordance with international standards. States also have a positive obligation to promote conditions that are conducive to freedom of expression and protect individuals from disproportionate interference by private entities.

It is with these parameters and considerations in mind that ARTICLE 19 developed the following recommendations.

7

Recommendations

This report has mapped the complex, fragmented landscape governing domain suspensions: from ICANN's narrow technical definition to registries' widely varying DNS abuse policies; from jurisdictional tensions to the absence of transparency requirements and due process mechanisms.

Three findings stand out:

1. The spectrum of DNS abuse definitions creates systemic vulnerability

Some registries stick to ICANN's technical definition while others supplement it with content categories ranging from CSAM to 'defamatory' or 'contrary to public policy' speech. There are also some who operate without clear definitions at all, deciding on a case-by-case basis. Because registries define DNS abuse differently, suspension requests made on the same grounds can result in different responses depending on where they were submitted. This inconsistency is not just confusing: it directly determines which speech stays online.

2. Registries operate under growing, often conflicting pressures

Registries must navigate ICANN contracts, national laws, court orders, law enforcement demands, and their own terms and conditions, all while often lacking legal clarity about their responsibilities. Some governments are wielding domain suspension as a convenient enforcement tool, and writing vague legislation that implicates domain operators 'by default'. This phenomenon is global. New EU regulations use domain takedowns to enforce financial regulation – and, concerningly, are doing so without conducting human rights impact assessments. When it comes to domain name suspensions a 'one-size-fits-all' approach does not work: such a blunt force tool requires careful consideration before use. At the same time, registries' governance structures, from their institutional ties to governments to their internal decision-making processes, shape how they respond to these pressures in practice. This means that their responses are highly variable, including in their ability or willingness to respect freedom of expression.

3. Registrants' rights often remain an afterthought

Most registries provide limited transparency about suspensions and virtually no appeals mechanisms. Registrants are often unaware that their domains were suspended, much less why or by whom. This transforms domain suspension from a legitimate and proportionate enforcement tool for terms and conditions or domestic laws into a potentially unchecked mechanism for censorship.

Together, these three realities create a dangerous dynamic: **attempts to moderate content through infrastructure-level entities are expanding rapidly without the safeguards that would protect free expression.** The cases from India, Spain, Nicaragua, and Belarus show that this is not a hypothetical problem. Journalists and human rights organisations are being silenced through domain suspensions, often without warning or justification. Especially when suspension orders come directly from the government, those impacted have limited to no recourse available.

But what if that could change?

The DNS was designed as an open, decentralised infrastructure that **enables access** to information **rather than restricting access** to content. Yet that is precisely what it risks becoming.

Protecting free expression at the infrastructure level requires action at every layer: from clearer definitions to due process mechanisms to strategic resilience-building.

The recommendations that follow address all stakeholders in this ecosystem:

- **Registries and registrars** who make suspension decisions;
- **ICANN**, which sets baseline standards;
- **Governments** writing legislation that implicates DNS operators; and
- **Civil society organisations** navigating these threats to their speech.

Our recommendations aim to balance the pressures that registries and registrars face to 'do something' about DNS abuse and the very real safety and security risks associated with it, while upholding freedom of expression.

Registries and registrars

1 Uphold human rights responsibilities in accordance with the UN's Guiding Principles on Business and Human Rights

Infrastructure providers, including domain operators, have a responsibility to respect human rights. Registries and registrants can do this by establishing recourse mechanisms to allow those impacted by DNS abuse mitigation action to contest domain suspension decisions, implementing transparency requirements for DNS abuse mitigation-related action (such as regular reporting on the types of domain suspension requests received by the domain operator and the outcome of such requests), and integrating appeal and dispute mechanisms.

2 Clearly define DNS abuse

Terms and conditions must establish a clear definition for abuse. Regardless of whether the registry/registrar opts to align with ICANN's DNS abuse definition or to expand its definition to a broader set of categories, having a definition clearly laid out in its contracts and easily accessible to registrants is paramount. This definition must have a clear scope of application; be limited to easily identifiable, replicable behaviour; and be consistently applied. Resources such as the framework to address DNS abuse can support registries and registrars who are looking to amend their current DNS abuse definitions to align with or productively build upon ICANN's strictly technical definition.

3 Assess DNS abuse reports on a case-by-case basis

Domain operators must assess DNS abuse reports on an individual basis. This starts with having a clear and consistent procedure for identifying the type of reported DNS abuse and confirming the validity of the report. Only once an investigation has taken place and a report of DNS abuse has been confirmed can the domain operator determine a course of action that is proportional to the abuse at hand. The Internet & Jurisdiction Policy Network's Toolkit: DNS level action to address abuses supports DNS operators in developing procedures, including questions to guide and structure decision-making.

4 Implement escalating mitigation response procedures

The decision to suspend or delete a domain is not a 'yes or no' answer. An escalating response procedure accounts for a sliding scale of options available for the registry, which goes beyond simply jumping to suspend or delete a domain. It also provides the registry with more time to contact the registrant and investigate further. Options include starting with a temporary suspension pending further investigation and contacting the registrant to see whether the issue can be addressed via an actor 'closer to the source' of the issue (such as going to the hosting provider or content publisher in cases with content-related issues).

5 Enshrine transparency as a key operating principle in internal operations

Transparency in internal policies entails how registries and registrars define DNS abuse, as well as the processes and procedures for responding to domain suspension requests. In practice, this means domain operators should ensure that their Terms of Service are sufficiently clear, accessible, and in line with international standards on freedom of expression. They should also provide more detailed examples or case studies on how their DNS abuse policies are implemented in practice. Where technically feasible, the addition of DNS extended error codes and/or landing pages to provide more information as to why a domain is inaccessible is another means of integrating transparency and building trust with end users. See NIC Chile's Reportes de Abuso/Abuse, auDA's Compliance posture, Cloudflare's Our approach to abuse, and PIR's Anti-Abuse Principles for examples of such documents.

6 Enshrine transparency as a key operating principle in external reporting

Publishing transparency reporting on DNS abuse mitigation action can build trust with registrants and the broader public. Reports should include information on the number and types of domain suspension requests within the reporting period, the reasoning behind decisions on these requests, the number of appeals processes and outcomes, and the actions the registry or registrar has taken to mitigate negative impacts on human rights, including freedom of expression. Some ccTLDs already publish such reports, such as the ccTLD operator for the Netherlands (.nl), SIDN. Beyond the EU, examples include Cloudflare's Transparency Reports and PIR's .org Anti-Abuse Metrics.

7 Commit to establishing recourse and redress mechanisms

These mechanisms must be consistent, transparent, and accessible. Registrants should be able to dispute a domain suspension by tracing the steps that led to the decision to suspend. This means that decisions should be made known, accessible, and understandable for all stakeholders. Additionally, as a default, registrants should be notified when their domain is the subject of a DNS abuse allegation or suspension order *even when the domain operator is not legally required to provide this information* (bearing in mind that there may be cases where this is legally prohibited or not otherwise possible given specific circumstances). See PIR's Anti-Abuse Policy Appeals Process and Cloudflare's Human Rights Commitments for examples.

8 Conduct public consultations when amending policies or terms and conditions

Since registries' terms and conditions are often pivotal in deliberations about whether to suspend a domain, the public should have the opportunity to understand and respond to changes in these documents. The ccTLD registry operators for Ireland, Australia, and the UK among others all provide examples on how to integrate public consultation into registry and registrar policy development processes (PDP).

9 Develop accessible resources to increase understanding of what domain operators can and cannot do

Suggested topics include how internet infrastructure works, information on how to file DNS abuse reports, and explanations of the operator's processes for addressing complaints. This not only serves the interests of registrants by providing clarity and transparency but also shields the domain operator from requests that are outside its remit or from DNS abuse reports that cannot be processed due to missing information. Punktum dk (ccTLD registry for Denmark) and SIDN (ccTLD registry for the Netherlands) both provide resources on how to file reports of abusive activity.

ICANN

10 Firmly reiterate ICANN's human rights commitments

ICANN's bylaws clearly state that ICANN is not a content regulator, and it has committed itself to safeguarding human rights in its policy development. This commitment should be top of mind in ICANN's policymaking process. **Committing to integrating human rights impact assessments throughout PDPs, rather than only in the inception of a PDP, is an easy way to uphold this commitment.**

Since 2025, ICANN has required a human rights impact assessment when a new PDP is launched; however, how this assessment is conducted and at what stage(s) of the PDP it should take place remains open to questions. The launch of ICANN's first working group on DNS abuse mitigation in March 2026 (of which ARTICLE 19 is a member representing the non-commercial stakeholder group) presents an opportunity to integrate human rights impact assessments *throughout* the PDP.

11 Standardise due process and recourse mechanisms

ICANN must develop a Consensus Policy on standard dispute and recourse mechanisms for registrants impacted by DNS abuse mitigation actions. The aim should be to set standards that enlist Contracted Parties in protecting the rights of internet users and domain holders.

Due process safeguards include establishing accessible complaint mechanisms, transparency requirements for DNS abuse mitigation actions (both in terms of the decision-making process and outcomes), and processes for reinstating domains when the abusive activity(ies) has been resolved (or when a suspension order was implemented in error). This recommendation was first put forward in NetBeacon's White Paper: Proposal for PDPs on DNS Abuse, and ARTICLE 19 reiterates its support for prioritising the topic for a PDP to develop Consensus Policy.

Governments

12 Protect, respect, and fulfil human rights

States have the ultimate responsibility to uphold international human rights. When it comes to the DNS, this means ensuring that users have mechanisms to assert their rights in relation to domain operators and to hold them accountable for domain suspension decisions and other DNS abuse mitigation actions. With respect to such orders, governments must ensure there are clear due process mechanisms for registrants. This includes ensuring there are accessible recourse and redress mechanisms available, such as pathways for reinstating domain(s) once the DNS abuse has been addressed or if domains were erroneously suspended. Such mechanisms must guarantee registrants' right to an effective remedy for violations of freedom of expression by domain operators.

13 Conduct human rights impact assessments when developing regulation requiring the use of domain suspensions

Governments must ensure that any legislation using domain suspensions (or 'deletion' or 'takedown') as an enforcement mechanism complies with international human rights law. Human rights impact assessments must pay particular attention to the impact of domain suspensions on freedom of expression, and the strict requirements under the three-part test of legality, legitimacy, and necessity and proportionality.

14 Clearly stipulate parameters for domain suspension orders

The circumstances for which a domain suspension is applied must be limited, evidence-based, and clearly delineated in the law. Registries and registrars cannot and should not be tasked with judging the legality of content found on their domains. Only courts or similar independent authorities should decide whether domain-level action on 'illegal' content is warranted. Governments should, at the very least, conduct a proportionality assessment in the PDP to safeguard against overreach. Prior to being issued, domain suspension orders must also be assessed individually for their potential human rights impact.

15 Integrate public consultations when developing legislation that could implicate internet operators

The aim should be to assess how legislation will impact human rights *before* adoption. Additionally, expert input helps to assess whether a domain suspension is the right course of action, or whether another actor with more precise technical capabilities and/or is closer to the content (such as a hosting provider) is better suited to address the issue at hand.

16 Clearly define policies pertaining to or impacting the DNS

Vague definitions, or unclear regulatory scope (in terms of which actors are responsible for implementing the legislation) can lead to overreach in suspensions, potentially rendering protected speech inaccessible. Consulting with technical and civil society experts will help with this. Additionally, where regulation mandates the use of domain suspensions as an enforcement mechanism, governments must clearly lay out the legal grounds for suspension and clearly demonstrate that these grounds have been met prior to enforcing the suspension. Domain suspension requests must only be issued by authorised entities, and requests must be assessed individually to ensure compliance with the standards of necessity and proportionality.

17 Develop capacity-building programmes

Governments should commit to providing technical training for policymakers who work on digital issues, particularly when it comes to the DNS. Policymakers working on internet policy must have a basic understanding of how internet infrastructure works to ensure that domain operators are not burdened with requests that lie beyond their technical abilities to act.

18 Recognise the varying roles of internet operators and their remit when addressing online content

As a rule of thumb, the registry or registrar should *not* be the first point of contact for removing problematic or abusive content from the internet. Domain operators are only able to suspend an entire domain, a measure that is also likely to affect content that constitutes protected expression. Given the risks for freedom of expression, DNS operators should not moderate content except as a last resort and under the strict limitations outlined in this research.

Civil society

Proactive action for civil society

19 Gather relevant information pertaining to the registry or registrar's policies

Civil society organisations – including independent media outlets – at risk of censorship should know their registry (and registrar, if applicable) ahead of time. Organisations at risk should prioritise registering their domain(s) with a registry or registrar that is transparent about its suspension policies and has clear and accessible recourse and remedy mechanisms in place.

20 Consider the jurisdiction of the registry when registering a domain name

Civil society organisations that operate in a country whose ccTLD registry operator has close ties to the government and are at risk of censorship should **pre-emptively register with a trusted registry based in another country**. Preference should be given to a gTLD registry operator because these must comply with ICANN's contractual obligations. Registries located in jurisdictions with robust protections for politically sensitive speech should be prioritised.

21 Regularly back up all content on websites and email servers

This will prevent the organisation from losing access to its contacts and content should there be a need to register a new domain and create new email addresses for staff.

22 Decentralise the organisation's domain operator services and email services

Decentralising systems, from email services, domain operator services, and intranet platform, protect the organisation from losing access to its internal and external communications when targeted with a domain suspension order.

23 Consider the contact information shared with the registry when registering the domain(s)

Having personally identifying information on file or publicised may put the registrant at risk. Depending on the respect for human rights in the organisation's operating environment, the personal safety of the registrant should be a priority. Where registering anonymously is not possible (such as in the EU), special attention should be paid to the data protection legislation (or the lack thereof) within the registry's jurisdiction.

Reactive action for civil society

24 Inform partners and networks as soon as a domain has been suspended or seized

This is to protect contacts in the organisation's network from responding to emails that are no longer under the organisation's control.

25 Contest domain suspensions through appeal mechanisms

To the extent that this is possible and safe in the local context, organisations targeted by a domain suspension order for the suspected purposes of censorship must make use of any available recourse or appeal measures. Where the registry or registrar does not have an easily accessible process internally for disputing a suspension (or has no process at all), turning to state or international human rights mechanisms is an option.

26 Develop a plan ahead of time for moving online resources to a new registry

In cases where it is not possible to reverse a domain suspension order (or it is not safe to appeal the decision), the targeted organisation should migrate its domain(s) to a different registry. The organisation should prioritise gTLDs or trusted ccTLD registries that demonstrate strong accountability mechanisms, clear and consistent communication with registrants, and transparent reporting practices.

27 Develop a rapid response advocacy campaign

Organisations experiencing censorship by means of domain suspension should seek out media coverage by larger news outlets and/or by censorship watchdog organisations, such as ARTICLE 19, the Internet Freedom Foundation in India, Citizen Lab, or the Open Observatory of Network Interference (OONI), among others. Where it is safe to do so, the objective should be to inform end users of the website's fate and to build up support for protective measures that allow the internet to remain a safe space for free expression.

Endnotes

1 Gillespie, T. (2018) *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven, CT: Yale University Press; and van Geuns, S. and Cath-Speth, C. (2020) 'How Hate Speech Reveals the Invisible Politics of Internet Infrastructure', 20 August.

2 In the context of this report, 'domain operators' refers to both registries and registrars.

3 See ARTICLE 19's 2023 reports: Tightening the Net: Iran one year on from the Mahsa Jhina Amini uprising' and 'Techtonic: Internet shutdowns as a tool of control'.

4 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, A/HRC/35/22.

5 Domain operators were selected to ensure diversity in geographic region, size, entity type (non-profit, private company, independent organisation, or foundation), and internal governance structure. Civil society organisations were selected to ensure diversity in geographic regions and to highlight the severity of the impact of DNS-level censorship.

6 VPNs allow users to access websites even if they are blocked in a specific location.

7 See OONI (2021) 'Introduction to Internet Censorship'; ISOC (2025) 'Policy Brief: Perspectives on Internet Content Blocking', 4 September; ICANN Security and Stability Advisory Committee (2012) 'SAC 056: SSAC Advisory on Impacts of Content Blocking via the Domain Name System', 9 October; ICANN Security and Stability Advisory Committee (2025) 'SAC 127: DNS Blocking Revisited', 16 May.

8 This concern was raised by multiple interviewees.

9 A more detailed breakdown of the actors in the DNS ecosystem can be found in CENTR's 'Domain name registries and online content'.

10 i2C, 'DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet', 2025.

11 Legitimacy here means that restrictions are only permitted for (a) the respect of the rights or reputation of others and (b) the protection of national security or public order, or of public health or morals.

12 See ARTICLE 19's reports 'Tightening the Net' and 'Techtonic'.

13 With phishing being a clear exception here as it involves content hosted on the domain.

14 Since 2025, Nicaragua has been led by the Government of Co-Presidents Daniel Ortega and Rosario Murillo. Ortega previously served as President in 1984–1990. He then returned to the presidency in January 2007, and his wife, Rosario Murillo, became his running mate and Vice President in January 2017.

15 See ARTICLE 19's coverage of the UK's Online Safety Bill and the EU's Digital Services Act.

16 Examples include streaming pirated content or the dissemination of CSAM, among others. Registries define illegal and illegitimate content differently, as discussed in Chapter 4.

17 For more on the different actors within the DNS ecosystem and their functions, see CENTR's guide 'Increasing Consumer Protection Online: The role of intermediaries in addressing infringing content'.

18 CENTR also uses this exact phrase in its guide on the role of intermediaries in addressing infringing content.

19 The GAC is an advisory committee to the ICANN Board. Its role is to advise ICANN on issues of public policy.

20 Registrars and registries must adhere to the obligations in their ICANN Contracts (Registrar Accreditation Agreement or Registry Agreement, as applicable). One of those requirements is to also follow obligations set out in Consensus Policies. A Consensus Policy is developed through the multistakeholder model of internet governance with input from groups throughout the ICANN Community.

21 Examples include .auDa's 'Compliance approach', Cloudflare's 'Our approach to abuse', and PIR's Anti-Abuse Principles.

22 This applies only to registries and registrars operating as private companies. Registries integrated into government ministries (only applicable to ccTLDs) have more stringent human rights obligations, as outlined earlier in this chapter.

23 Punktum dk's terms and conditions set out in detail the registry's decision-making process for suspending a domain name. Both the ccTLD registry operators for Ireland and the UK delegate the decision-making process for domain suspension when it comes to reports of CSAM to external watchdog organisations – Hotline and the Internet Watch House Foundation, respectively.

24 More information on landing pages for DNS operators can be found here.

25 Shapiro, M. N. (2025) 'Looking Ahead: ICANN's Upcoming Policy on DNS Abuse Mitigation,' 12 December; NetBeacon Institute (2025) 'White Paper: Proposal for PDPs on DNS Abuse'.


ARTICLE19