Consultation on a Modern Copyright Framework for Online Intermediaries

Submission of the Canadian Internet Registration Authority

Canadian Internet Registration Authority (CIRA)

#400, 979 Bank Street

Ottawa, On K1S 5K5

May 31, 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Canadian Internet Registration Authority (CIRA) is a member-based, not-for-profit organization best known for managing the .CA top-level domain (TLD) on behalf of all Canadians. This work includes maintaining the .CA domain name system (DNS) and associated registry services.

CIRA has long championed the principles of an open internet, which are essential to ensuring that the internet's different components interoperate effectively, and is opposed to impingements on it, such as what might occur with site blocking at the internet service provider (ISP) level. Under the principle of net neutrality, the content of internet communications are not controlled or interfered with by intermediaries except in extraordinary circumstances without a reasonable alternative to achieve a pressing outcome. In considering site blocking as a remedy for copyright infringing activities, it should therefore be unavailable unless:

a) other reasonable remedies targeting intermediaries closer to the infringing activity have proven ineffective;
b) the site's electronic location and locus of control are deemed to operate outside of Canada and, therefore, beyond the reach of direct enforcement;
c) blocking is implemented in a way that, in the view of an impartial third party competent to review such matters, is least harmful to the quality, efficiency, and security and stability of the internet as a telecommunications network;
d) and a fair and considered process overseen by a court of competent jurisdiction testing the use of these other remedies has been followed.

To this end, CIRA is seeking a number of changes and clarifications to the proposals set out in the *Consultation on a Modern Copyright Framework for Online Intermediaries.* Our concern is primarily focused on the proposals set out in 4.4.1, "Establish a Statutory Basis and Procedure for Injunctions Against Intermediaries":

> *The [Copyright] Act could be amended to provide expressly for injunctions against intermediaries to prevent or stop online copyright infringement facilitated by their services even where they are not themselves liable for it, such as where they may be protected by the safe harbours. These injunctions could be available through a court process to ensure the highest standards of procedural fairness. The specific relief possible through such injunctions could include orders to disable access to infringing content (e.g., "website-blocking" or "de-indexing" orders), remove such content (e.g., "takedown" orders), otherwise prevent or stop infringing activity (e.g., "stay-down" orders) or limit, suspend or terminate access to an intermediary's service.*

The proposal seems to suggest that all of these options have equal merit or efficacy, or ought to be weighed equally, in addressing the problem of infringement. This is not the case. The most logical and effective way to proceed initially is against the owner or operator of the site. Where

that bears no reasonable chance of success, as may be demonstrated by unsuccessful efforts undertaken in good faith, the next most effective method is to seek an injunction against the website hosting provider to have the content itself removed — what the consultation paper calls a "takedown order." The involvement of the financial services and online payments communities may also be useful. Consequently, the scope of what might be considered an intermediary should be expanded to include these communities.

The more invasive option of website blocking at the ISP level strays from copyright-only matters to encompass the subject-matter of the *Telecommunications Act.* Blocking is, in fact, only a partial remedy as it is easily circumvented by, for example, obtaining a new domain name, or by users employing a commercial virtual private network (VPN) service or alternative public DNS resolver which does not filter out the website in question. Finally, if implemented incorrectly at the network layers, as there are multiple ways of doing this, website blocking may have unexpected negative consequences.[1] [2]

Given the limitations of site blocking, the proposed statutory guidelines should make it clear that a website blocking order cannot be issued unless the copyright owner has established a *prima facie* case of commercial scale infringement, they have failed to secure redress from the website owner, and efforts to have the hosting provider remove the content have been unsuccessful. Site blocking should only occur where both the site owner and hosting provider are located outside of Canada, thus outside the jurisdiction of a Canadian court, and where the hosting provider refuses to honour a Canadian order for injunctive relief. Should the department of Innovation, Science and Economic Development Canada (ISED) seek to allow for website blocking orders, the Government of Canada should follow the practice of Australia[3] and only permit these where the infringing content is located outside of Canada.

The issue of content abuse online is receiving considerable attention internationally and there are emerging best practices in this area. CIRA commends ISED's attention to the work of the Internet and Jurisdiction Policy Network which recently published a toolkit entitled *DNS Level Action to Address Abuses.*[4] It contains a proposed "content complaint referral path" which integrates the important principles of necessity, proportionality, transparency and non-discrimination into a progressive approach to content abuse mitigation. This progressive approach lays out a hierarchy of different online intermediaries and the order in which to involve them when addressing issues of content abuse online.

---

[1] Internet Society, "Internet Society Perspectives on Internet Content Blocking: An Overview", *Internet Society*, March 24, 2017, https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[2] Security and Stability Advisory Committee, "SAC 056: SSAC Advisory on Impacts of Content Blocking via the Domain Name System," ICANN Security and Stability Advisory Committee, October 09, 2012, https://www.icann.org/en/system/files/files/sac-056-en.pdf

[3] Copyright Act 1968, (Cth), No 63/1968, s 115A(1)., http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ca1968133/s115a.html

[4] Internet and Jurisdiction Policy Network, "DNS Level Action to Address Abuses," *Internet and Jurisdiction Policy Network*, March 2021, https://www.internetjurisdiction.net/domains/toolkit

The *Copyright Act* currently contains no definition of what might constitute an 'online intermediary', though the consultation document provides a casual definition, that being "the entities that facilitate access to the immense and growing volume of online content." Later, the document indicates that intermediaries include internet service providers, private data storage services, web hosting and related services and web-based messaging, calling or mail services, among others. What is notably absent from this list is DNS operators when many, if not most, instances of website blocking are carried out through intervention points within the DNS. This omission suggests that the paper's authors may not be fully aware of the important role played by various DNS operators in the architecture of the internet.

Internet access is a telecommunications service which is governed by the *Telecommunications Act*, which in turn has a number of policy objectives that strive to ensure the availability of high-quality affordable services and to enhance competition in the industry. Directing smaller ISPs to implement website blocking may prove to be a financial burden, thus impacting competition in the industry. It is of concern that the consultation document does not reference the *Telecommunications Act*, its policy objectives, common carriage (AKA "net neutrality") obligations, and the potential impact on competition, or specifically engage telecommunications stakeholders.

This is even more peculiar given that s. 36 of that Act specifically prohibits service providers from interfering with content transmitted across their network. These telecommunications policy issues need to be surfaced and debated before proceeding. The timeframe for this consultation has been quite short, indeed rushed. CIRA is of the view that more research and background study is required before proceeding.

CIRA remains opposed to the concept of website blocking at the ISP level as, in all but the most extreme circumstances, it violates the principles of net neutrality that underwrite a free and open internet, and the common carriage principles codified in the *Telecommunications Act.* Should the government introduce a statutory framework for injunctive relief to address copyright infringement among online intermediaries, website blocking should only be permitted to address commercial-scale infringement after all other available remedies have proven ineffective, a fair and considered process overseen by a court has been followed, the infringing content's electronic location and locus of control have been determined to be outside of Canada, and the blocking order has been implemented in a way that is the least harmful to the security and stability of the internet. CIRA requests further consideration of these issues before any legislative amendments are proposed.

INTRODUCTION

The Canadian Internet Registration Authority (CIRA) is a member-based, not-for-profit organization best known for managing the .CA top-level internet domain name on behalf of all Canadians. This work includes maintaining the .CA domain name system (DNS) and associated

registry services. CIRA is also responsible for developing and implementing policies for the .CA domain that support Canada's internet community, and representing the .CA registry internationally.

CIRA has long championed the principles of an open internet to ensure that the internet's different components operate together in an effective and standards-based manner. In an open internet, the content of internet communications between endpoints are not controlled or interfered with by intermediaries except in extraordinary circumstances where reasonable, more proportionate alternatives are unavailable. This ensures that any user of the network can expect their information to reliably reach its destination free from interference by intermediaries.

CIRA has significant expertise in network operation and internet governance, having participated in multiple regulatory and legal proceedings about intermediary liability as it pertains to website blocking. CIRA is also a member of several international domain name industry working groups on international telecommunications, security, and internet governance issues.

Most pertinent to this proceeding is our participation in the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet & Jurisdiction Policy Network (I&JPN). ICANN is the California-based not-for-profit corporation responsible for global coordination of, and policy on, the unique domain names and Internet Protocol (IP) addresses that bind the internet together as a network of networks. The I&JPN is the preeminent multistakeholder organization dedicated to understanding the mechanisms to address online abuse in a cross-border context. Its secretariat facilitates a global policy process engaging over 400 entities including governments, internet companies, technical operators, civil society groups, academia and international organizations from over 70 countries.[5]

Drawing on this expertise, our submission will focus on the enforcement tools and obligations of intermediaries to address copyright infringement. The submission will detail how the internet works as a hierarchy of technical functionalities performed by different types of service providers. It will then identify enforcement actions available at each stage of functionality, and their corresponding consequences for internet users.

The consultation document proposes establishing a statutory basis for injunctions against intermediaries, including mechanisms to disable access to infringing content, such as “website-blocking,” or “de-indexing.” These mechanisms exist at different layers within the internet’s staged hierarchy of technical functionalities. We submit that any remedy established in legislation that would require domain name registries to suspend domains or internet service providers (ISPs) to block websites is a remedy of absolute last-resort, after a step-by-step approach of progressive escalation has been duly exhausted. We propose a “referral path” for

[5] Internet and Jurisdiction Policy Network, “About,” *Internet and Jurisdiction Policy Network,* Date Accessed May 28, 2021, https://www.internetjurisdiction.net/about/mission

content abuse, including copyright abuse that is rooted in the principles of necessity, proportionality, transparency, and non-discrimination.

CIRA does not function as a content host or platform. This submission will therefore not address the question of remuneration schemes as contemplated by the consultation document.

ABOUT CIRA

The .CA DNS and Registry

In the DNS, a top-level domain (TLD) is the part of a domain name that appears to the right of the dot; for example, COM, NET, CA, UK, or BIZ. There are over 1500 TLDs available. The authoritative list of all TLDs is maintained by the Internet Assigned Numbers Authority (IANA) in the Root Zone Database, overseen by ICANN. A country-code top-level domain (ccTLD) is generally used and reserved for a country, sovereign state, or territory as identified with an International Organization for Standardization (ISO) 3166-1 alpha-2 country code. Canada's ccTLD is .CA.

CIRA's responsibility to manage the .CA top-level domain and the underlying authoritative DNS services arises from the management function extended to CIRA in the 1999 letter from the Government of Canada.[6] ICANN and IANA recognize CIRA as the authoritative TLD manager for the .CA ccTLD. CIRA is responsible for ensuring the uniqueness of domains in the .CA zone and maintaining the authoritative directory of domain names therein. There are now more than 3 million .CA domain names, which CIRA has registered.

As a domain name registry, CIRA operates an information system ("database") whose zone files contain the resource records that are the single authoritative source of information for .CA domain registrations. This authoritative database is distributed across many locations and updated regularly, for resiliency. These records amount to what some describe colloquially as the .CA "phonebook," or official records on where to find a given .CA domain on the internet. At the core, CIRA and its TLD registry perform a directory function. As such, TLD registry operators do not have influence over the content of websites, nor do they transmit or store the content of websites.

Persons who wish to register a .CA domain name, called "registrants," do not deal directly with CIRA. Instead, they must deal with a CIRA-certified "registrar." Registrars are organizations certified by CIRA to facilitate the registration, transfer, renewal and modification of registration data for registrants. Only CIRA-certified registrars may apply to CIRA for the registration of domain names in the .CA registry and request modifications and other transactions with respect to .CA domain name registrations (for example transfers, renewals, etc.) pursuant to agreements, policies, rules and procedures set by CIRA and agreed to by the certified registrars.

[6] Michael Binder, "Letter from Michael Binder, Industry Canada, to Robert Hall, CIRA," *IANA,* March 11, 1999, https://www.iana.org/reports/2000/ca-report-01dec00/industry-canada-letter-11mar99.html

For example, the registrant of the domain name *Canada.ca* is Shared Services Canada using the registrar Authentic Web Inc.[7] Authentic Web registered the domain name in the .CA registry with CIRA on behalf of the registrant, Shared Services Canada. The Government of Canada's primary contractual relationship for the domain name is with Authentic Web Inc. In registering a domain through Authentic Web, the government also enters a contract with CIRA and agrees to abide by CIRA's terms of service.

It is important to note that neither CIRA, as the registry, nor Authentic Web, as the registrar of the domain name, have any control over the content the government makes available on *Canada.ca.* The content resides on the premises of web hosting providers. As we will discuss later in the submission, neither suspending the domain name with the registrar or registry, nor blocking the domain at the ISP level would directly affect the content itself. Even if *Canada.ca* was suspended or blocked, sophisticated users would still be able to access this content by using tools such as virtual private networks (VPNs) or alternative DNS resolution services. It is therefore most effective and proportional to remove the offending content at the web-hosting level.

CIRA'S Relevant Experience

How to curb copyright infringement online is not a new policy debate. CIRA has participated in regulatory, judicial, and policymaking proceedings about intermediary liability as it pertains to site blocking. Most recently, CIRA intervened in *TekSavvy Solutions Inc. v. Bell Media Inc. et al* at the Federal Court of Appeal to assist the Court in the determination of factual and legal issues related to the appeal.[8] CIRA's priorities in this intervention were to protect the technical integrity of the DNS and internet architecture from problems associated with website blocking at the ISP level, to help the Court appreciate deficiencies in the Plaintiffs' approach in this matter, and to suggest preferable alternatives.

CIRA also made submissions to the government-appointed panel responsible for conducting the Broadcasting and Telecommunications Legislative Review in 2019.[9] CIRA's submissions centered on the technical arguments for continued separation of broadcasting and telecommunications legislation. Communications law in the digital age, CIRA submitted, should attempt to regulate at those points on the internet most directly associated with the related policy objectives.

---

[7] CIRA, "WHOIS: The domain canada.ca is registered," *Canadian Internet Registration Authority,* Date Accessed May 28, 2021, https://www.cira.ca/ca-domains/whois?domain=canada.ca

[8] Memorandum of Fact and Law of the Intervener, Canadian Internet Registration Authority and of the Intervener, The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, *TekSavvy Solutions Inv v Bell Media Inc., et al,* 2020 FCA No. A-440-19, https://www.cira.ca/sites/default/files/2020-08/A-440-19_CIPPIC-CIRA_Intervener_Factum.pdf

[9] CIRA, "Submission to the Broadcasting and Telecommunications Legislative Review Panel," *Canadian Internet Registration Authority*, January 11, 2019, https://www.ic.gc.ca/eic/site/110.nsf/vwapj/979_CanadianInternetRegistrationAuthority_4d_EN_CA.pdf/$FILE/979_CanadianInternetRegistrationAuthority_4d_EN_CA.pdf

In addition, CIRA made submissions to the Canadian Radio-television and Telecommunications Commission (CRTC) in response to the 2018 site blocking proposal by Fairplay Canada.[10] CIRA opposed the Fairplay proposal on the grounds that website blocking by ISPs should only be permitted in exceptional or extreme circumstances due to the potential for unintended harm caused by relying on the DNS to block content, and to the ability of users to circumvent such blocking mechanisms.

CIRA participates in international working groups dedicated to developing new methods and industry best practices for curbing technical and content abuses online. These include ICANN meetings, where CIRA staff have served in various ICANN leadership positions to foster policy consensus and technical cooperation among ccTLDs, as well as facilitate the development of best practices for ccTLD managers globally. In 2012, the ICANN Security and Stability Advisory Committee published an advisory report about the impacts of content blocking, including site blocking, via the domain name system.[11] The report outlines issues that governments should take into consideration in order to fully understand the technical implications of different methods of site takedowns or site blocking when developing policies that depend upon the DNS to block or otherwise filter internet content.

CIRA also participates in the I&JPN, described earlier, which has a mandate to enhance legal interoperability and reduce jurisdictional tensions in the global governance of the internet. CIRA staff are currently involved in a working group which considers issues of jurisdiction related to domain names and the DNS, specifically including questions about how the neutrality of the internet's technical layer can be preserved when national laws are applied to the DNS.

Our submission will draw on CIRA's submissions to related proceedings, best practices within the internet governance communities in which CIRA participates, and the efforts of the domain name industry to address abuse.

OPTIONS FOR REFORM AS CONTEMPLATED BY THE CONSULTATION PAPER

Section 4.4 of the consultation document contemplates clarifying or strengthening the tools available to rights holders in their online enforcement efforts, with a focus on commercial-scale infringement. The document goes on to propose the establishment of a statutory basis and procedure for what it refers to as "website blocking," "de-indexing," or "takedown" orders in the form of court Injunctions against intermediaries.

[10] Canadian Internet Registration Authority, Intervention in Public Process 8663-A182-201800467 - Asian Television Network International Limited, on behalf of a Coalition (FairPlay Canada), Application to disable on-line access to piracy sites. https://services.crtc.gc.ca/Pub/ListeInterventionList/Documents.aspx?ID=272608&en=2018-0046-7&dt=i&lang=e&S=O&PA=T&PT=A&PST=A

[11] Security and Stability Advisory Committee, op. cit.

CIRA agrees that statutory guidance is required for the courts to interpret the appropriateness of such remedies for rights holders. Other jurisdictions base blocking orders on explicit statutory regimes. Where legislators prescribed statutory benchmarks, such as in Australia, the United Kingdom (UK), and elsewhere in the European Union (EU), courts grant blocking orders in accordance with the relevant statute. Australian legislation is "deliberately prescriptive; it is intended as a precise response to a specific concern raised by copyright owners."[12] CIRA agrees that within the framework of an explicit statutory regime, courts are the appropriate body to determine what constitutes copyright infringement and to order intermediaries to take action, provided that when such orders engage other areas of the law such as telecommunications, they are tested against those policy goals and issued in the manner that best furthers them.

Canadian jurisprudence on website blocking is limited. *Bell Media Inc. et al v Goldtv.biz et al., (2019 FC 1432)* ("GoldTV") saw the court acting without explicit statutory guidance, instead relying on a body of case law from outside Canada and efforts to read between the lines of the *Telecommunications Act* and the *Copyright Act.* The major flaw in the GoldTV approach is that a court has granted an injunction, not as a last resort, but as a first resort. Moreover, it has done so in a context where there is evidence of Canadian operators and information potentially available from Canadian entities, and from financial intermediaries, and whose efficacy or availability were not first tested by the court. For example, the plaintiffs did not make efforts to seek an injunction or a *Norwich* order with the content hosts, the domain name registrars or registries, or the payment processors.

CIRA submits that a new statutory basis for online copyright enforcement efforts should indeed be codified, and in a way that the extreme remedy of site blocking at the ISP level would be a true last resort. Instead of site blocking as a first resort, as we see in the GoldTV jurisprudence, CIRA makes submissions about developing a logical and hierarchical referral path of intermediaries that are best suited to address the infringing content.

The reforms as proposed by the consultation paper suggest that all options for enforcement have equal value in addressing the problem of copyright infringement. Given the limitations of website blocking, new statutory guidelines should make clear that a site blocking order cannot be issued unless and until the copyright owner has tried and failed to secure redress from the website owner and efforts to have the hosting provider remove the content have also failed. Finally, the latter situation should only occur where both the site owner and hosting provider are located outside of Canada, thus outside the jurisdiction of a Canadian court, and where the hosting provider refuses to honour a Canadian order for injunctive relief.

DNS ABUSE

The DNS has been likened by many to the internet's address book. When a user enters a domain name in an internet browser—Canada.ca for example—the browser is configured to

[12] Australia Commonwealth, Senate, Copyright Amendment (Online Infringement) Bill 2015, Revised Explanatory Memorandum, (2015), ¶1.

access one of the many nameservers owned and operated by CIRA (located in Canada and around the world) to tell the user's computer the internet protocol (IP) address of the server where the content managed by Canada.ca is located. Put simply, the registry helps match the domain name to its unique, corresponding number (IP address) "out there" on the network. CIRA's role in the process is the same as other TLD registries, including other country code TLDs (ccTLDs) such as .fr, .us, .uk, .de; and generic TLDs (gTLDs) such as .com, .net, .org. The role of a registry is to maintain records of registrants and provide the IP address where the content can be located via authoritative DNS resolvers. The content itself, however, is located on servers operated by hosting providers. DNS resolvers do not host any content, nor does any internet content travel over the DNS itself.

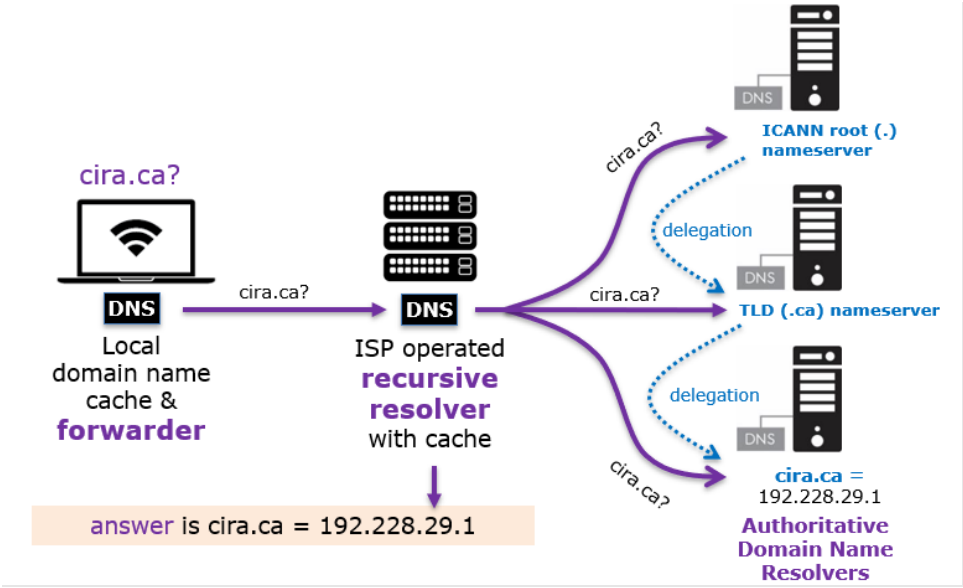


Figure 1. *How a domain name is resolved*

ISPs provide what are called recursive DNS services to their customers, but this is ancillary to their provision of internet connectivity. The recursive DNS services of ISPs are largely unseen and unfelt by the end user but are necessary to the provisioning of internet connectivity services. As demonstrated in *Figure 1*, the recursive DNS records of ISPs rely upon the authoritative records of ICANN and the TLD registries. There are also many standalone DNS resolver operators in Canada that are neither domain name registries nor ISPs. These also rely on the records of ICANN and TLD registries. DNS resolvers play an essential role in how internet users access websites and in how intermediaries implement site blocking, yet the technology is curiously absent from the consultation document.

DNS operators from around the globe, such as registrars and registries, are, from time to time, presented with orders compelling domain name suspensions or registrant identification details related to alleged abusive content on the sites underlying their domain names. The domain name and internet governance communities have identified two major categories of DNS abuse: technical abuse, and website content abuse. An associated set of best practices is emerging for addressing each category. The I&JPN defines these categories as:

a) Technical abuse (e.g. phishing, malware distribution, etc.), which is closely related to the security and stability of the technical layer of the internet; and
b) Content abuse (e.g. child sexual abuse imagery, intellectual property violations, etc.) which occur at the level of the website

Copyright infringement is therefore categorized as a type of content abuse. Technical abuses and content abuses each present different sets of characteristics and considerations for online intermediaries. Content abuse, including copyright abuse, is best dealt with through content-proximate intermediaries such as social media platforms and web hosting providers. The DNS, as an addressing system or directory function, is a neutral technical infrastructure which is critical to the proper functioning of the internet. Similarly, ISPs function as neutral common carriers of telecommunications. Intervention at these layers is an invasive and blunt way of addressing content abuse, and should not be reached for as the first logical tool for doing so, for reasons we outline below.

The I&JPN offers helpful guidance for establishing a referral path hierarchy for content abuses which takes into consideration the specialized roles and categories of various internet intermediaries. They propose a process of procedural due diligence organized around the closeness of the relationship of the intermediary to the person or entity sharing the infringing content. The proximity of that relationship also determines the precision with which the intermediary can take action to remove the content. A toolkit for *DNS Level Action to Address Abuses* is available on the I&JPN website.[13]

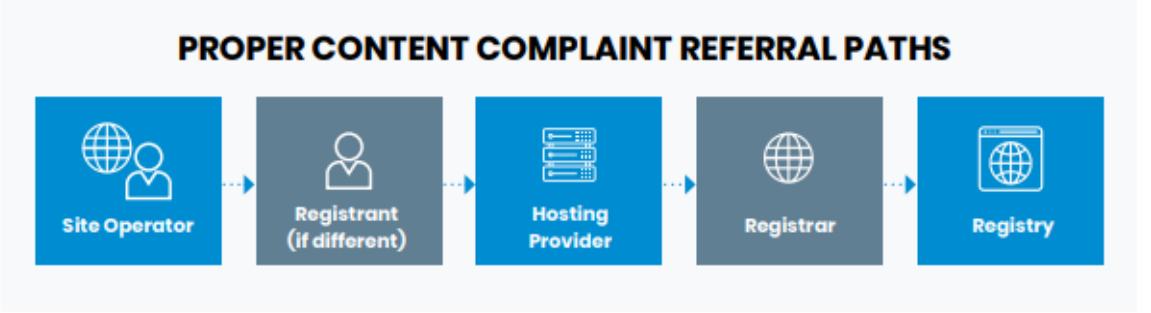


Figure 2. *Proper Content Complain Referral Paths, Internet and Jurisdiction Policy Network*[14]

CIRA supports the model of a referral path of procedural due diligence for addressing the problem of online copyright infringement, which includes both internet intermediaries and the financial services intermediaries who facilitate the electronic transfer of funds that incentivizes online infringement.

CIRA submits that intervention at the ISP level should be a remedy of absolute last resort which, unlike other remedies considered, engages the *Telecommunications Act* in addition to the

[13] Internet and Jurisdiction Policy Network, "DNS Level Action to Address Abuses," *Internet and Jurisdiction Policy Network*, March 2021, https://www.internetjurisdiction.net/domains/toolkit
[14] Ibid, 15.

Copyright Act. What is more, acting at the DNS or ISP level for website content abuses should only be considered when a domain is used with clear intent of significant abusive conduct, and only after other, more effective, and more narrowly-tailored remedies have been exhausted through a defined course of procedural due diligence.

PRINCIPLES

The next sections of this submission establish why a defined referral path of procedural due diligence is the appropriate approach for a framework that addresses copyright infringement. CIRA submits that such a referral path must be rooted in the principles of necessity, proportionality, transparency, and non-discrimination, which we understand to be international best practice. The provisions of the EU Open Internet Regulation establishing net neutrality rules across Europe to be enforced by national telecommunications regulatory agencies, for instance, state in part:

> Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.
> The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.
>
> Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary…[15]

CIRA urges the Government of Canada to adopt as foundational to the modernization of the copyright framework for online intermediaries the principles of transparency, non-discrimination, necessity, and proportionality underlying a referral path of escalating measures to address copyright infringement online.

[15] Eleni Vytogiannni and Marnix Dekker, "Guidelines on assessing security measures in the context of Article 3(3) of the Open Internet regulation", *European Network and Information Security Agency (ENISA)*, December 2018, p. 4. https://doi.org/10.2824/94531

Necessity

Before persons or entities filing complaints alleging abuse seek remedies with intermediaries operating in the technical infrastructure of the internet— including domain registrars, domain registries, and ISPs—they must conduct proper substantive and procedural due diligence. Substantively, there must be no question as to the substance of the allegation, that is, the infringement is unequivocally piracy and not a 'fair use.' The rights holder must ensure any claim against the content of a domain is properly investigated, substantiated and documented (e.g., screen shots, evidence of ownership in claims of infringement.) Only after this proper substantive due diligence has been undertaken would the process of addressing the abuse through procedural due diligence be commenced. CIRA commends the statement in the consultation document that the focus of any new regime for orders would be on commercial scale infringement rather than infringement by individuals. Commercial scale activity would need to be established at this stage.

This procedural due diligence would follow the content complaint referral path outlined earlier, starting with the intermediary whose relationship is closest to the person or entity sharing the infringing content. The I&JPN's proposed 'Proper Content Complaint Referral Path' provides excellent guidance on the order in which a rights holder should provide notice.[16] The government may also contemplate injunctions against financial intermediaries, such as payment processors, and other intermediaries involved in the chain of value.

In assessing whether it is necessary to grant a blocking or takedown injunction at the ISP level, the court must determine whether such a blunt enforcement tool is necessary under the circumstances. Under Australia's statutory scheme for site blocking, only "an online location outside Australia" can be blocked.[17] This "important limitation on the power of the Court", wrote Australian Justice Nicholas, "may reflect an assumption that other provisions of the Act provide copyright owners with adequate remedies in respect of online locations situated within Australia".[18] This is to say, more proportional remedies than site blocking targeting intermediaries closer to the infringing content are available to the court when the site operator or hosting company is situated in and subject to the jurisdiction of the court. It is therefore unnecessary to seek redress at the ISP level when other more appropriate and more effective interventions are available in the court's jurisdiction.

Proportionality

Any remedial action sought through intermediaries must be proportionate to the severity of the infringement. First, the damage must be significant in the context of the injunctive relief sought. The proportionality of the effects on intermediaries must also be considered.

On one side of the proportionality fulcrum is a spectrum of copyright enforcement options, ranging from least to most intrusive. On the other side are an array of economic impacts,

[16] Internet and Jurisdiction Policy Network, op. cit. 15.
[17] Copyright Act 1968, (Cth), No 63/1968, s 115A(1).
[18] Roadshow v Telstra (2016 Decision) [2016] 122 IPR 91.

human rights, public interests, internet governance, and technical and policy considerations. The balance point between these is the principle of minimal impairment. Less intrusive options should be tried first. The most intrusive option (blocking) should be ordered last.

For example, *facebook.com* would not be ordered taken down by a registry or registrar, or blocked by ISPs, because a small percentage of posts by its users contains infringing content. Such an order would make the entirety of *facebook.com* unavailable to most people, and skip more proportionate approaches. Indeed, in this situation, it's clear that the intermediary with the ability to remove the content with precision and the least impact on the technical functioning of the internet is the site operator: Facebook Inc.

In the case of a file sharing site, if a registrar or registry suspended the domain due to a small proportion of infringing content then thousands of other pieces of legitimate content such as open-source software or Creative Commons-licensed media would be rendered inaccessible by users. Similarly, an individual's personal website should not be ordered taken down or blocked because a small percentage of the content infringes upon a rights holder. The intermediaries with the ability to remove the content with precision are the website operator or registrant and the website hosting provider, who are likely able to remove the instances of abusive content while leaving the remaining content (and the domain name) intact.

Furthermore, as mentioned earlier, intervening in the DNS is rarely completely effective as many takedown or blocking techniques can be circumvented by sophisticated users employing VPNs, alternative DNS resolvers, or the IP address underlying a given domain name.

Ordering a website be blocked by ISPs is a blunt instrument that crosses statutory domains, requires coordinated action by many different network operators, challenges net neutrality, and can have collateral impacts. In CIRA's view, direct action at the DNS level is only justified in the context of technical abuse, because of the imminent threat to the security and stability of the internet. For content abuse, acting at the DNS level is rarely appropriate as DNS operators are not in a position to remove the offending content. At these intervention points, the whole of the site would become unavailable, including those portions that include non-offending material. Furthermore, services such as email that rely on the resolution of a domain name, may also become inoperable.

However, if the rights holders have pursued a path of procedural due diligence and demonstrated the website operator and website hosting companies are non-responsive and the process has escalated to the registrar and registry level, the next step is an in-depth evaluation towards making a decision on whether the abuse meets a sufficient threshold justifying taking action at the DNS level.

Even if it is established that the website contains infringing material, the proportion of the site dedicated to the infringing content must be considered. It would not be appropriate to seek to block access to Tik Tok or Facebook because of isolated instances of copyright infringement.

Caution would also need to be taken with respect to file sharing sites where the majority of the content is non-infringing.

Even if it is found that some form of action at the DNS level is warranted, a further decision is required on the specific action to be taken. Action at the DNS level can take the form of holding a domain so that it does not resolve, locking the domain, transferring or even deleting it.[19] [20]

Transparency

Some of the most internationally recognized guidelines for designing legal frameworks for intermediary liability come from the Manila Principles on Intermediary Liability, which were designed through a multi-stakeholder process in 2015. The sixth of the six Manila Principles calls for programmatic transparency with respect to content-oriented blocking ("[t]ransparency and accountability must be built into laws and content restriction policies and practices"). The following guidance is particularly germane:

> c) Intermediaries should publish their [blocking] policies online, in clear language and accessible formats, and keep them updated as they evolve, and notify users of changes when applicable….
> e) Intermediaries should publish transparency reports that provide specific information about all … restrictions taken by the intermediary, including actions taken on government requests, court orders, private complainant requests, and enforcement of … policies.[21]

Any framework for addressing copyright related content abuses that employs content takedowns or website blocking as a remedy must include mechanisms for notifying the infringing party that they have offended, and notifying users attempting to access the content what content has been ordered taken-down or blocked and on what grounds. In the absence of such transparency, DNS blocking can be misdiagnosed and may result in responses from end users, network administrators, service providers, etc. that attempt to mitigate the damage.[22]

As a best practice, intermediaries should publish their corporate policies for compliance before the fact, and account for how they have been applied afterwards. Finally, there must be a publicly available appeal mechanism where the website owner can contest the action. This is particularly important in cases of false positives, where infringement is inappropriately identified or applied.

[19] Internet and Jurisdiction Policy Network, "DNS Level Action to Address Abuses," pp. 18-23.
[20] Security and Stability Advisory Committee, op. cit. 8-9.
[21] "Manila Principles on Intermediary Liability," March 24, 2015, p. 4 https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf
[22] Security and Stability Advisory Committee, op. cit. 6.

Non-Discrimination

Independent judicial oversight is a key consideration given the vertically-integrated nature of Canada's telecommunications sector, where several major players have significant content holdings and sell internet services. There is an issue of negative competitive impact that must be assessed in considering telecommunications policy concerns with the vertical integration of common carriers and content providers. In the GoldTV case, the applicants seeking the remedy were also the third-party common carriers tasked with implementing it.

As stated by a 2019 Parliamentary committee considering blocking orders: "It is not hard to imagine a situation where one vertically integrated ISP-rights-holder seeks an injunction that would apply to another ISP-rights-holder, who would gladly provide it with little contest given that they share similar interests in the outcome of the case."[23] In clarifying intermediary liability and developing a framework for enforcement of copyright, parliament must seize the opportunity to clarify how to weight such difficulties against polycentric telecommunications and copyright objectives.

WHO IS AN INTERMEDIARY?

The *Copyright Act* contains no definition of what constitutes an 'online intermediary'. It is unclear which actors this consultation aims to capture or provide clarity around. DNS operators, including domain name registrars and registries, as well as public DNS resolver operators are not contemplated by the consultation. DNS operators' absence is notable because the consultation document proposes a statutory framework for takedowns and website blocking — remedies that are achieved by utilizing intervention points within the DNS. Consulting on website blocking without understanding the DNS is like studying the behavior of the tides without understanding the patterns of the moon.

CIRA has interventions in policy that are available to rightsholders in order to address alleged abuses, including copyright infringement. Rightsholders may contact the registrant of a domain name. For domain names owned by businesses, rightsholders can complete a WHOIS search to obtain the contact details for the registrant. The contact details of individuals who own domain names, however, are protected for privacy reasons and not searchable through WHOIS. If one wishes to contact an individual registrant, they may use CIRA's message delivery form, which enables the rightsholder to send a message to the registrant.[24] This is a tool that allows rightsholders to send notices to registrants and ask for the infringing content to be removed, a first step in the content complaints referral path described above.

In the event that the owner of a domain name does not respond to the message sent through CIRA's message delivery form, CIRA has rules and procedures for the Request for Disclosure of

[23] Canada, Parliament, House of Commons, Standing Committee on Industry, Science, and Technology, *Statutory Review of the Copyright Act,* 42nd Parliament, 1st Session, pp 97-98.
[24] CIRA, "Contact a domain holder: Message Delivery Form," *Canadian Internet Registration Authority,* Date Accessed May 27, 2021, https://www.cira.ca/ca-domains/contact-a-domain-holder

Registrant Information.[25] To be able to request information, Requestors must meet the following requirements:

a) the information is not publicly available through the WHOIS search tool,
b) the Requestor must have a good faith dispute with a registrant, meaning the Requestor reasonably believes in good faith that the domain name or its content infringes their (I) registered trademark, (ii) registered copyright, (iii) issued patent, (iv) registered corporate, business, or trade name, or
c) is making use of the Requestor's personal information without their knowledge or consent to commit a crime.

This process enables a rightsholder to engage with registrants in good faith in order to try to address alleged copyright infringement at the party closest to the infringement – the registrant. The omission of the DNS from the consultation document suggests the paper's authors may not be fully aware of the important role played by DNS operators in the architecture of the internet, and therefore as intermediaries that may be captured by proposed updates to the *Copyright Act.*

It is also unclear why the consultation is restricted solely to so-called "online intermediaries," when other points of interventions or "choke points" exist. CIRA notes that financial intermediaries, such as payment processors like PayPal, or credit card companies, which play a key role in much infringement, and have material information of assistance in identifying the infringing party, are absent from this list.

Finally, the *Telecommunications Act* governs the provision of telecommunications services. It is concerning that the consultation document does not refer to the *Telecommunications Act,* its policy objectives, the principle of common carriage or net neutrality, or how the proposed enforcement tools for online copyright infringement could impact the body of law and regulation that form telecommunications policy in Canada. These telecommunications policy issues need to be raised and considered before proceeding. CIRA holds the view that more research and background study is required before proceeding.

CONCLUSION

The reforms proposed in the consultation paper for modernization of Canada's copyright framework for online intermediaries suggest that site blocking and takedown orders are the preferred enforcement tools. We have demonstrated that there are more effective, less intrusive, and more proportional enforcement tools that exist which target intermediaries closer to the infringing activity.

[25] CIRA, "Request for Disclosure of Registrant Information," *Canadian Internet Registration Authority,* Date Accessed May 28, 2021, https://www.cira.ca/policy/rules-and-procedures/request-disclosure-registrant-information

An intellectual property owner who believes that their copyright has been violated should seek redress through the use of a progressive and proportional process that begins with the owner of the website and then through the hosting provider. CIRA urges the Government of Canada to adopt a referral path of escalating measures to address copyright infringement online. Such a framework would be rooted in the principles of transparency, non-discrimination, necessity, and proportionality, and would harmoniously integrate the objectives of both the *Telecommunications Act* and the *Copyright Act.*

Website blocking should only be considered a measure of last resort to be used after working through the remedies available closer to the infringing content. Only after these remedies have been exhausted without redress should a rights holder seek action at the DNS or ISP level. When remedy is granted here, it must be proportional to the degree of harm posed by the site. Rarely, and only under extraordinary circumstances, is it justified to block a whole domain name.

Finally, the lack of clarity around what constitutes an intermediary; the omission of a concurrent consideration of the relevant elements of the *Telecommunications Act;* and the timing of the appellate court's decision on Canada's only site-blocking jurisprudence all point to the need for more time and study before the implementation of a statutory scheme for site blocking.

APPENDICES

A. Security and Stability Advisory Committee, “SAC 056: SSAC Advisory on Impacts of Content Blocking via the Domain Name System,” ICANN Security and Stability Advisory Committee, October 9, 2012

B. Internet and Jurisdiction Policy Network, “DNS Level Action to Address Abuses,” Internet and Jurisdiction Policy Network, March 2021

C. Michael Binder, “Letter from Michael Binder, Industry Canada, to Robert Hall, CIRA,” IANA, March 11, 1999

D. Memorandum of Fact and Law of the Intervener, Canadian Internet Registration Authority and of the Intervener, The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, TekSavvy Solutions Inv v Bell Media Inc., et al, 2020 FCA No. A-440-19

E. CIRA, “Submission to the Broadcasting and Telecommunications Legislative Review Panel,” Canadian Internet Registration Authority, January 11, 2019

F. CIRA, Intervention in Public Process 8663-A182-201800467 - Asian Television Network International Limited, on behalf of a Coalition (FairPlay Canada), Application to disable on-line access to piracy sites

G. CIRA, ”Request for Disclosure of Registrant Information,” Canadian Internet Registration Authority

H. Manila Principles on Intermediary Liability, March 24, 2015

APPENDIX A

SAC 056

SSAC Advisory on Impacts of Content Blocking via the Domain Name System

An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)

09 October 2012

Preface

This is an Advisory of the Security and Stability Advisory Committee (SSAC). The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this Advisory, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this Advisory, are at end of this Advisory.

Table of Contents

1. Executive Summary

The use of Domain Name System (DNS) blocking to limit access to resources on the Internet has become a topic of interest in numerous Internet governance venues. Several governments around the world, whether by law, treaty, court order, law enforcement action, or other actions or agreements, have either implemented DNS blocking or are actively considering doing so. However, due to the Internet's architecture, blocking by domain name can be easily bypassed by end users and is thus likely to be largely ineffective in the long term and fraught with unanticipated consequences in the near term. In addition, DNS blocking can present conflicts with the adoption of DNS Security Extensions (DNSSEC) and could promote balkanization of the Internet into a country-by-country view of the Internet's name space.

This document is limited to an exploration of technical impacts related to DNS blocking including:

- Domain blocking via:
  - A registry or registrar;
  - An authoritative server;
  - In a recursive resolver via redirection, non-existent domain name, a query refused response code, other response codes, or a query non-response.
- DNS blocking in recursive resolvers and conflicts with DNSSEC;
- Conditioning end users toward more end-to-end encryption;
- Over-blocking;
- Typographical errors;
- Routing DNS traffic away from a nation that imposes blocking;
- Impacts of users switching resolvers; and
- Breaking Content Distribution Network (CDN) localization if users switch resolvers.

While there are also non-technical issues such as limitations on freedom of expression, these issues will not be addressed in this document. The Internet community, governments, and others should ensure that they understand and carefully consider all of the issues related to DNS blocking, both technical and non-technical.

2. Introduction

This document builds upon "SAC050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee," which may be of interest to readers of this document.[1]

In 2011 and 2012 several governments proposed or established formal guidelines, laws, court orders, or law enforcement actions related to DNS blocking, DNS filtering, and/or domain name seizure.[2] In some cases the objective of these activities was to develop new legislation aimed at controlling Internet usage, while in other cases courts or law enforcement agencies have relied on DNS blocking or domain name seizures as a mechanism to block access to certain Internet sites or addresses.[3,4,5,6]

This document examines the technical impacts of various types of DNS blocking that have been implemented or proposed. The aim of this paper is to inform the Internet community, policymakers, government officials, and others of the high-level technical implications of using the DNS blocking to control access to Internet resources.[7]

3. DNS Blocking: Benefits Versus Harms

The major conclusions of SAC050 are:

> "Domain name or Internet Protocol (IP)-address based filtering (or preventing access to for example web content that infects computers with viruses or are deemed an inappropriate use of employer resources) may be viewed by some organizations as a

---

[1] See "SAC050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System," Internet Corporation for Assigned Names and Numbers (ICANN), Security and Stability Advisory Committee, 14 June 2011, http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

[2] See H.R. 3261 (Stop Online Piracy Act), United States House of Representatives, 112th Congress, version dated December 16, 2011 and Estonian law regarding blocking of illegal gambling sites, https://www.riigiteataja.ee/akt/125042012010.

[3] See OpenNet Initiative, http://opennet.net/youtube-censored-a-recent-history.

[4] See http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] See http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] See http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] For a description of the DNS see http://queue.acm.org/detail.cfm?id=1242499

> natural extension of historical polices that block people within those organizations from incurring telephone toll charges.
> …
> Regardless of the mechanism used, organizations that implement blocking should apply these principles:
>
> 1. The organization imposes a policy on a network and its users over which it exercises administrative control (i.e., it is the administrator of a policy domain).
> 2. The organization determines that the policy is beneficial to its interests and the interests of its users.
> 3. The organization implements the policy using a technique that is least disruptive to its network operations and users, unless regulations specify certain techniques.
> 4. The organization makes a concerted effort to do no harm to networks or users outside its policy domain as a consequence of implementing the policy.
>
> When these principles are not applied, blocking using the DNS can cause collateral damage or unintended consequences with limited or no remedies available to affected parties."

To expand on the conclusions of SAC050, both due consideration and overall Internet stability require that any DNS blocking policy or action be fully disclosed to affected parties including end users, service providers, and application designers. DNS blocking in the absence of such disclosure will lead to unnecessary troubleshooting activities as well as adaptive and perhaps even unintended bypass activities by network operators and end users. Such disclosures should include motivations, intended effects, and expected side effects. Absent such transparency, DNS blocking can be misdiagnosed as an outage or as a malicious attack and may result in responses from end users, network administrators, service providers, etc. that attempt to mitigate the damage.

This potential for misdiagnosis and the inevitable search for workarounds can result in collateral damage or unintended consequences. Independent public review was also called for in the Office of the United Nations High Commissioner for Human Rights Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression which states:

> "31. […] Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a

judicial or independent body."[8]

An exploration of the types and impacts of DNS blocking is the subject of the remainder of this document.

4. Blocking Content in the Context of the Internet's Architecture

One of the fundamental tenets of the Internet architecture is its 'end-to-end' abstraction, which minimizes the need for intelligence in the core (middle) of the network but embraces intelligence at the edge (on individual hosts). This architecture has enabled a tremendous range and depth of innovation by, for example, allowing a developer at one edge of the network to deploy a new application on a host and an end user at the other edge to install a corresponding client enabling new forms of communication, without requiring any special permission or controls within any other part of the network.

Content blocking via the Domain Name System has been implemented sometimes in the Internet "core" and sometimes at the Internet "edge." Connections between an access provider and its traffic sources and traffic sinks are called "edge." Connections inside or between operators are called "core." Examples of edge-based blocking would include black lists in web browsers and filtering IP traffic at one end of a connection. If edge-style blocking were applied in the network core, affected end users could bypass the blockage by changing DNS providers or by using VPNs, proxies, or plugins. Edge-style DNS blocking will only be effective where policy-based filtering is present in all possible paths between affected end users and any networks with which they might exchange packets. Examples of such topologies include national and enterprise firewalls.

As a side effect of this architecture, efforts to block traffic, whether by domain name (such as example.com) or by IP address (such as 192.0.2.117), at any point in a network other than at the edge *can be circumvented*, for example by the use of a virtual private network (VPN).[9] VPNs and similar methods are readily available and easy to adopt by even relatively unsophisticated users. Even in cases where complete administrative and operational control over Internet access networks is possible (such as within an Internet Service Provider (ISP) or at some Internet exchange points[10]), end users have still been able to access prohibited

[8] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A.HRC.17.27., http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[9] See http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html or http://vpn-account.com/bypassblockedsites.html.

[10] See http://en.wikipedia.org/wiki/Internet_exchange_point.

content.[11]

The common characteristic of these more successful types of filtering is that the end user and her network operator agree explicitly or implicitly to what is filtered and how the blocking of content is done. In this case, the end user sees DNS blocking as a valuable service.

5. Types of DNS Blocking Observed or Proposed

Various methods of blocking DNS have been proposed or implemented in recent years. Some methods pose greater technical concerns than others. A non-exhaustive list follows:

1. **Domain Seizure via a Registry or Registrar**: This method removes DNS data from its source via a DNS registry or registrar acting as the registry's agent. A registry is the entity responsible for creating the authoritative database of DNS data including the domains to be blocked. An example of this method would be a government serving a domain name "take-down" order to a registrar or registry who is lawfully subject to such an order. A registry or registrar's response to such a take-down demand depends on the specifics of the order. Options include removing a domain name from the zone (known as a "domain hold" when the registration data for that domain is maintained) thereby preventing end users from resolving a domain name associated with a specific site, or mapping the domain name to a different nameserver that will then redirect users to a web page displaying additional information such as law enforcement notices of the take-down. In the "domain hold" situation, once the domain's DNS record's "Time To Live" (TTL) settings expire, usually over the course of a few hours or days, the domain becomes unresolvable globally. This means that when a user types in that domain name, a "domain does not exist" response will be returned. If the correct domain names are seized, there are no direct negative technical implications unique to the "domain hold" method. Indirect negative technical implications can include failures in distant services if other domains depend for name service or e-mail service or web service on the domain subject to such a "hold". In either the "domain hold" or name server change method, the registrar or registry must also update or remove any DNSSEC data for the targeted domain. Failure to do so would cause DNSSEC-compliant applications to detect invalid data in responses to DNS queries that would prevent any communication at all, even to explain to users why the domain was no longer available.
2. **Domain Blocking in an Authoritative Server**: This type of blocking, implemented by the operator of the authoritative name servers of the affected domain name, bypasses the registry and possibly also the

[11] See http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

registrar, and targets directly the mechanism by which the domain name is made available on the Internet. Once a registrant has obtained and correctly configured a domain name, the registry generates the DNS data and publishes that data to a set of "authoritative servers." In many cases the registrar operates these authoritative servers, but this is not a requirement, nor is it a requirement that all of a domain's authoritative servers be operated by the same entity. Regardless of who operates the authoritative servers, the servers are a publishing mechanism and are therefore a point at which DNS blocking can be implemented. An example of this form of blocking would be a government serving a domain name take-down order to an operator of a DNS server that is authoritative for the targeted domain name. That operator would then remove or modify their copy of the authoritative DNS records for that domain name. Assuming the take down order was sent to and implemented by all operators of authoritative servers for the domain, the domain would become immediately unreliable on a global basis and eventually unresolvable after the TTL of the domain's DNS records expires. In addition to different entities implementing the blocking, this method differs from registry/registar-based blocking in that it can create difficulties if DNSSEC is in use since the authority server operator may not be able to preserve the registry's DNSSEC signatures when altering registry domain content.

3. **Domain Blocking in a Recursive Resolver**: Recursive resolvers are a common place to implement DNS blocking with a number of tools (both commercial and open source) that allow resolver operators to easily implement blocking.[12] However, due to the DNS architecture, blocking in a recursive resolver is among the most easily bypassed. Recursive resolvers, typically operated by the end user's ISP, fetch DNS data from authoritative servers on request from end users. When an end user wishes to connect to a web site or other service, the recursive resolver serving that end user translates the domain name of that site or service into IP addresses. DNS blocking via recursive resolvers aims to filter, edit, or block this translation and can be done in a number of ways:

    a. **Via Redirection**: In this form of recursive resolver blocking the response from the authoritative server is modified to substitute values specified by the DNS blocking policy. For example, instead of returning the IP address of the offending web server, the recursive resolver returns an IP address of a remediation server that

[12] See http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ and http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

displays a message indicating the site is being blocked.[13]

This form of blocking requires the remediation server to support any protocols or services supported by the original target servers for which displaying a redirection banner is technically possible. That is, if the target of the blocking is using the File Transfer Protocol (FTP) to provide content, the server to which the user is redirected must also use FTP in order to display the banner.[14] Due to the way some protocols work, this type of redirection may not be feasible in all cases.[15] However for common protocols such as Hypertext Transfer Protocol (HTTP, the core protocol for the World Wide Web), this kind of redirection is achievable.

b. **Via a Non-Existent Domain Name (NXDOMAIN) Response Code**: As with redirection, this form of blocking modifies the response from the authoritative server; however instead of returning the IP address of another server, the response is modified to indicate the requested domain does not exist.

c. **Via a Query Refused Response Code**: The DNS protocol has a response code, REFUSED, which is intended to signify that a domain is not resolvable for administrative reasons. DNS blocking can be implemented by changing the response from an authoritative server to a REFUSED response for blocked domains.

   One perfectly valid and reasonable interpretation of the DNS protocol specification is that REFUSED response codes indicate the name server should not be queried at all, which may result in the operating system removing that recursive resolver from its list of name servers. This is because the REFUSED response is interpreted as an access control problem for the client and for all domain names requested by that client, rather than as a refusal to answer for some specific domain name. With a sufficient number of end user queries, this type of blocking could result in all of the name servers used by the end user being removed, rendering the end user's computer being unable (or unwilling) to query any name. Thus, resolvers returning REFUSED for a domain being blocked are likely to result in unacceptable collateral damage.

---

[13] See http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] See "File Transfer Protocol" at http://en.wikipedia.org/wiki/File_Transfer_Protocol.

[15] See "Redirection in the COM and NET Domains (9 July 2004)", ICANN Security and Stability Advisory Committee at http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

d. **Via Other Response Codes:** There are additional response codes specified in the DNS protocol that can be used to signal that a domain is not resolvable, usually indicating some sort of error has occurred. These response codes include "server failure" (SERVFAIL), "not implemented" (NOTIMPL), and "format error" (FORMERR).

   As with REFUSED, blocking via these response codes may result in the operating system declaring the recursive resolver as non-functional and removing it from the list of recursive name servers the operating system queries. For this reason, none of these alternative responses are suitable for DNS blocking.

e. **Via Query Non-Response**: Finally, the recursive resolver could be configured to ignore queries for a requested domain. This may result in applications attempting to connect to the blocked site to reattempt the resolution through multiple query iterations.

   As with REFUSED and other error response codes, the operating system may remove the recursive resolver from its list of name servers it queries for any name (not just the blocked name). However, unlike blocking via the response codes described above, blocking by not returning a response results in a significantly worse end user experience since the application must wait for all of the lookups to time out. This may encourage users to change to alternate recursive resolvers, potentially using servers not covered by the takedown order or desired blocking policy.

Reconfiguring recursive resolvers is operating system dependent but typically requires a small number of clicks in the "System Preferences" graphical user interface, and many available 'apps' operating systems in general operating systems and smart devices alike make this a one-click process as well. In almost all cases, this reconfiguration is within the capabilities of all but the most non-technical users.

As mentioned earlier, blocking via recursive resolvers is a common form of DNS blocking in use today; however end users can bypass this form of blocking by using a recursive resolver that does not implement the blocking, e.g., an "open" resolver that accepts queries from any source IP address[16] or by running their own recursive resolvers.

In addition, since recursive resolver-based DNS blocking re-writes or modifies the DNS responses received from the authoritative servers, the

[16] Popular open resolvers include OpenDNS (http://www.opendns.com/) and Google Public DNS (https://developers.google.com/speed/public-dns/).

chain of trust model used by DNSSEC will be broken and DNSSEC-related errors will be generated. These errors may lead an end user to conclude that the DNS recursive resolver has a problem or is under attack. This conclusion would be credible because with DNSSEC, DNS responses rewritten under government mandate are technically indistinguishable from what may be observed during malicious cache poisoning.

6. Contrasting Authoritative or Registry-Based DNS Blocking with Recursive Resolver Blocking

Some countries, such as the United Kingdom taking action against names in the .uk TLD[17] or the United States taking action against names in the .com Top Level Domain (TLD)[18] have seized domain names that are maintained by a registry that operates within their borders. In some cases, the domain name was placed on registry hold; in other cases, DNS records were modified to direct traffic to a government-controlled web site.

Assuming that the blocked domain names are few in number and that it is not trivial or cost-free to create new domain names serving the same audience and the same purpose, domain name seizure can be effective in blocking Internet content. Since actions in a TLD are taken at the publication point all DNS recursive resolvers globally will usually have the blocked names removed within a relatively short timeframe, specifically within the TTL of the DNS records being blocked.

When domains are seized at the registry level, DNSSEC[19] continues to operate as intended since this action is a modification to DNS content at its source and thus, assuming the DNSSEC signatures are regenerated appropriately, the DNSSEC chain of trust is unbroken.

However, if the registry providing the names to be blocked is located in a different legal venue, cooperation of law enforcement or government officials in different jurisdictions may be required. This can be problematic in the cases where the other country's laws are incompatible, or the law enforcement organizations do not have explicit mutual legal assistance treaties, teaming agreements, cooperation or coordination agreements via for example Interpol. As such, registry level domain take-down is most practical within a single legal jurisdiction although improvements in the coordination and cooperation among law enforcement agencies have recently been visible. For example, cooperation may be achieved via law enforcement participation in the multi-stakeholder

[17] See http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] See http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] See http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

ICANN process, and by creation of special task forces within organizations like the creation of European Cybercrime Center (E3C) within Europol.[20]

DNS blocking at the authority server requires that each authoritative server operator makes changes to the zone it receives from the registry, without authorization by that registry. In the case where the authoritative servers are operated by more than one organization, this may be challenging. Should one or more authoritative server operators fail to reflect the same change within the same version of the zone, incoherent results could be returned for the same query depending on which resolvers were queried, which authoritative servers were queried by the resolvers, when the queries occurred, etc. Further, unless the authoritative server operator also happens to be the holder of the zone signing key (ZSK), the modifications to the zone made by the authoritative server operator would not be signed, thereby causing the DNSSEC chain of trust checks to fail for resolvers that do validation. As a result, this form of blocking tends to be impractical.

The use of recursive resolver-based DNS blocking avoids these jurisdictional issues since the take-down orders are addressed to ISPs or other resolver operators within the same legal jurisdiction of the body requesting the take down. The trade-off is that since various network operators all around the world operate recursive resolvers, it is impossible to ensure complete coverage without coordinated and universal data path filtering and payload manipulation. Additionally this would break in the face of end-to-end application-level DNSSEC validation, as discussed in the next section. However, at least one study has shown that because of a phenomenon called "upstream filtering" actions by an ISP in one country to filter or block content, may result in blocked content in another country because of routing arrangements among ISPs.[21] The unintended consequences of this sort of extraterritorial government influence could manifest as increased operating costs and decreased stability for all Internet operators and users.

7. DNS Blocking in Recursive Resolvers Conflicts with DNSSEC

As discussed in previous sections, the implementation of DNSSEC can have significant impact on DNS blocking activities. DNSSEC is a set of enhancements to the DNS protocol designed to address data authenticity issues within the DNS. Although DNSSEC-enabled applications are not yet in widespread use, the need for such applications is a key driver of the development and deployment of DNSSEC. End-to-end deployment of DNSSEC is required to enable support for

[20] See https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

[21] See https://citizenlab.org/2012/07/routing-gone-wild/.

cryptographic authentication in current and future security-sensitive applications, essential to safeguarding the public's trust in the global Internet.

Effective DNS blocking via recursive resolvers conflicts with the purpose and operation of DNSSEC. This is because DNSSEC is designed to detect exactly such changes that blocking intends to introduce, although the term "blocking" implies that the change itself is made in accordance with legislation and/or other rules to which involved parties agreed. The changes that blocking produces are indistinguishable to the changes that DNSSEC makes detectable, such as criminals intentionally injecting false DNS responses so that traffic is redirected to false services. Any modifications made to DNSSEC-signed data look identical to malicious DNS poisoning attempts because there is no feature or signal within DNSSEC to tell a receiver that a given response has been signed by an authority other than the domain holder. This holds true for domain holds where the purpose is to simply black out a web site and also for domain redirections where the purpose is to display a government interception/take-down notice in place of the web site via redirection. In either case an end user's resolver when validating DNSSEC-signed responses will be able to tell that tampering has occurred but will not know the cause of that tampering. The end-user's resolver's actions when it detects this kind of tampering may include the use of workarounds, such as ignoring the local recursive resolver iteratively resolving the entire chain of trust from the root to the authoritative servers itself.

DNS blocking at the recursive resolver level can be a feasible if temporary stopgap. Specifically, if one were to block or filter DNS only when either the domain name holder or the end user did not use DNSSEC then the modified data would still be accepted by end user resolvers and used by applications such as web browsers. However the workaround for a domain holder who does not want their domain name to be blocked would be to sign their DNS data, and the workaround for end users who does not want their content blocked in this way would be to enable DNSSEC in their stub resolvers.[22] Thus the characterization, "temporary stopgap."

While it is often assumed that DNSSEC validation can or should only be done "in the network" this ignores the needs of DNSSEC-aware applications. DNSSEC can be used "in the network" to protect a DNS cache from poisoned data, and in the early years of DNSSEC deployment that is the only use the Internet industry can make of DNSSEC. However, the long-term vision for DNSSEC is to create an entirely new class of DNSSEC-aware end user applications using technologies such as DNS-based Authentication of Named Entities (DANE), an effort underway in the Internet Engineering Task Force (IETF).[23] The DANE working

[22] Stub resolvers are minimal DNS resolvers that use recursive query mode to offload most of the work of DNS resolution to a recursive name server. Almost all Internet devices contain a stub resolver, and almost all access networks provide a recursive name server to their customers. See http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] See https://datatracker.ietf.org/wg/dane/charter/.

group is now standardizing a mechanism by which the identity of a secure web server, and the security of the connection between a browser and that secure web server, is enhanced via DNSSEC rather than via the older and increasingly trouble-prone X.509 certificate authority network.[24]

As a result of efforts to use DNSSEC as a general infrastructure upon which secure applications will be built, it can be assumed that DNS blocking in recursive resolvers will either have a negative impact on DNSSEC deployment or become ineffective once DNSSEC sees broader implementation. The world's economy can either have secure Internet naming and therefore secure Internet applications, or have effective content blocking via Internet DNS – but not both.

8. Other Implications of DNS Blocking

DNS blocking and filtering carry potential implications beyond those discussed in previous sections. Some clear possibilities include over-blocking and bypass/circumvention by routing DNS traffic away from blocking enforcement points.

8.1 Over-Blocking

Under the assumption that DNS blocking techniques will be used, there is a risk that errors will occur in the list of entities to be blocked. This is independent of whether the blocking is based on domain names or other identifiers such as IP addresses or Uniform Resource Locators (URLs). Because of this fact, the processes used to review items to be added to a given list must be secure, trustworthy, and allow for extensive vetting. The lists used in the blocking examples described in this report derive from varied sources: private entities, cooperating law enforcement agencies, and courts or legislatures. The SSAC does not take a view on what process is best but recommends several mechanisms to promote technical stability: clear rules on what may be blocked, and a well-defined review and decision making process.

In addition, it is important to recognize that if blocking is implemented for a domain such as *example.com*, blocking using the domain name system will not only block the ability to look up the domain name when accessing content under the blocked URL *http://example.com/bad-content.html*, but also all other URLs using that same domain name; e.g., under *http://abc.example.com/* or *http://example.com/good-content.html*. DNS blocking will also block domain name lookup for all other services such as e-mail, network management, file transfer, etc. that use the same domain, and additionally, child domains of

[24] Examples of recent challenges with X.509 include the compromise of Diginotar (see http://en.wikipedia.org/wiki/DigiNotar) and multiple compromises as Comodo Registration Authorities (see http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

example.com (e.g., *subdomain.example.com*).[25]

Finally, in any filtering regime, whether in the DNS or elsewhere, it is vitally important to avoid errors in the generation of targets for blocking. For example a typographical error during data entry could both fail to block the intended domain name and accidentally block some unrelated domain. Internationalized domain names (IDNs) can pose special hazards since two IDNs can appear to be identical yet be distinct inside the DNS.

8.2 Routing DNS Traffic Away From a Nation That Has Imposed Blocking

Government action that results in domain blocking can encourage end users to take steps to ensure their DNS traffic is routed through name servers outside the country, for example by using VPNs or specific recursive resolvers instead of the ones operated by the access provider. This "off shore" routing of domain name queries can transfer DNS observability and control to other countries, frustrating anti-cybercrime activities within the country implementing blocking, and/or fostering increased cybercrime activities by entities outside of the country. In addition to additional latency that may be incurred, this external routing of DNS traffic can also have an impact on Internet performance within the blocking nation as many content delivery networks make decisions regarding what information to return on DNS queries based on the source IP address of the resolver making the query. The use of non-local servers can result in unexpected traffic traversing international links.

Changing to another name server, whether it is part of the common ICANN-coordinated DNS or an alternate system, can be done by straightforward rewriting of a computer's configuration, greatly facilitated by the existence of friendly graphical user interfaces on most computer systems today. Even if individuals do not have the requisite knowledge to modify their computer (or network) DNS settings, scripts and custom applications that automate DNS modification have been posted for download. An example is the MAFIAAFire plug-in posted after early stages of the U.S. Immigration and Customs Enforcement's Operation In Our Sites initiative.[26]

---

[25] See http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/, and http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

[26] See https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ and http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

8.2.1 Impacts of Users Switching Resolvers

DNS data give ISPs an important and accurate picture of both traffic patterns and security threats on their networks. This information can allow an ISP to identify increases and shifts in traffic, which can inform business decisions. Even more importantly, monitoring DNS data supports network security, often enabling ISPs to diagnose denial-of-service attacks and identify infected hosts, compromised domains, and vulnerable users.

As users increasingly turn to DNS servers other than those provided by their ISPs, those ISPs will have decreased ability to manage security threats and maintain effective network operations. The reduction of customer use of an enterprise, local network operator, or ISP's DNS service will mean that more compromised computers will go unidentified and uncorrected. Furthermore, the set of Internet configuration attributes that need to be evaluated when a customer calls an operator help desk for support will be much more extensive, and will increase both cost and debugging complexity.

The issues outlined above also will provide challenges for the governments of nations in which ISPs are located. Those governments may lose the ability to gain intelligence information through possible data sharing arrangements with network and Internet services operators, and also be without information that might be important evidence in law enforcement investigations. For example, the U.S. government might not have had sufficient evidence concerning botnet command and control structures and poisoned caches to have brought cases such as Operation Ghost Click, a significant action that shut down servers that propagated the DNSChanger malware.[27]

Law enforcement issues will be particularly acute when a user chooses a DNS server in another country. The ability of legal processes to address a problem is diminished when servers are out of the jurisdiction of a given enforcement agency.

8.2.2 Breaking CDN Localization If Users Switch Resolvers

Routing DNS traffic so that it does not match network topology, for example via DNS servers outside of a given country, also will negatively affect network performance (within the nation, per added propagation and aggregate round trip times) and increase costs for ISPs. For example, if users switch resolvers to avoid blocking the result may be that CDN localization may fail to work and the end user may be directed to content from CDN nodes hosted on servers outside of their country, rather than those located in the user's access network with direct interconnection links.

[27] See http://www.fbi.gov/news/stories/2011/november/malware_110911.

CDNs commonly localize content delivery by distributing the same content across servers on a wide range of networks globally. This localization reduces the load on any single server and minimizes network resource consumption and congestion by delivering content from servers as close to the user as possible. Many CDNs infer a user's location based on the IP address of their DNS resolver, which means users who have shifted to DNS resolvers outside their own country will appear to the CDNs to be browsing from abroad. The result will be a negative impact on performance and stability for such CDN users, and increased costs for ISPs transporting the associated traffic.

9. Conclusions and Further Reading

While blocking access to content via the DNS has become more common, both as a topic of study as well as in implementation, it carries with it a number of technical issues. Blocking at the DNS registry level (either directly or via a registrar) has the fewest technical implications and can work with DNSSEC but may run afoul of jurisdictional problems or trigger long-term balkanization of the Internet name space. Blocking at the authoritative servers has similar jurisdictional issues but cannot work with DNSSEC in the cases where the authoritative server operator does not also have the ability to correctly sign the zone containing the name(s) to be blocked. Finally, blocking at the resolver level, while common today, is at best problematic in the face of DNSSEC and at worst could impede the deployment of DNSSEC.

Governments and others should take these issues into consideration and fully understand the technical implications when developing policies that depend upon the DNS to block or otherwise filter Internet content.

Suggested further reading on this topic includes the following articles:

- *Shutdowns, Suspensions, Seizures, Oh My!*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.
- *Preventing Access or Removing Content – Laser Scalpel or Saw?*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- *A Chainsaw is a Poor Choice for Surgery and for Blocking Content*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.
- *Alignment of Interests in DNS Blocking*, P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

10. Acknowledgments, Statements of Interests, and Objections, and Withdrawals

These sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

10.1 Acknowledgments

The committee wishes to thank the following SSAC members and other contributors for their time, contributions, and review in producing this Report.

Alain Aina
Jaap Akkerhuis
Don Blumenthal
KC Claffy
David Conrad
Patrik Fältström
James Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Paul Vixie

10.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 Objections and Withdrawals

There were no objections or withdrawals.

APPENDIX B

DOMAINS & JURISDICTION PROGRAM

TOOLKIT

DNS LEVEL ACTION TO ADDRESS ABUSES

MARCH 2021
I&JPN REF: 21-105
www.internetjurisdiction.net/domains/toolkit

INTERNET & JURISDICTION POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

DESIGN & LAYOUT
João Pascoal Studio
www.joaopascoal.com

CITATION
Internet & Jurisdicion Policy Network Toolkit
DNS Level Action to Address Abuses (2021)

TABLE OF CONTENTS

1. ISSUE FRAMING

Cross-border requests for domain name suspensions are increasingly sent to Domain Name System (DNS) Operators in relation to alleged abusive content or activity on underlying websites.

Yet, the DNS, as an addressing system, is a neutral technical layer vital for the proper functioning of the internet. This level is neither a fully effective way - nor should be considered as the natural tool - to address abusive content. Protection of the core of the internet is and should be a key priority.

Acting at the DNS level should only be considered when it can be reliably determined that a domain is used with a clear intent of significant abusive conduct. Furthermore, because a domain suspension has by definition a global impact, the concept of proportionality dictates that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is also important that the actual impact of specific actions at the DNS level is well understood by all actors.

This important issue is generally recognized as outside of the Internet Corporation for Assigned Names and Numbers (ICANN) mandate. Moreover, the fundamental distinction between generic and country-code Top Level Domains (gTLDs and ccTLDs) in terms of relations with, respectively, ICANN and national laws or authorities, leads to very different approaches and constraints.

All actors are nonetheless confronted with a common challenge: defining when it is appropriate to act at the DNS level in relation to the content or behavior under a domain address, and what role courts and so-called "notifiers" should or could respectively play in that regard.

The Domain Name System (DNS), as the "phonebook of the internet", saves internet users the burden of memorizing Internet Protocol (IP) addresses. Thanks to the DNS, information can more easily be accessed online through domain names, for example: nytimes.com or lemonde.fr.

Importantly, the DNS exists and operates independently from the underlying websites or services where or through which abuses happen. Addressing abuses on the internet should not have negative impacts on the integrity and reliability of this essential infrastructure layer upon which internet use relies.

In that regard, it is critical to distinguish two categories:

1.) **Technical abuse** (*e.g.* phishing, malware distribution, etc.), which is closely related to the security and stability of the technical layer of the internet; and
2.) **Website content abuse** (*e.g.* child sexual abuse imagery, intellectual property violations, etc.) which occur at the level of the website.

Accordingly, what is often labelled as "addressing DNS abuse", should rather be understood as: "DNS level action to address abuses online".

DNS Level Action to Address Abuses

DNS Operators (registries and registrars - the entities that manage domain names) have limited technical options at their disposal to address abuses, which do not include the capacity of removing specific slices of content from websites. Moreover, when a DNS Operator takes action to disable a domain name, the underlying website and its content remain available through the website's IP address. These technical limitations coupled with the complex interplay of competing legal systems in varying jurisdictions often differ as to whether particular forms of content are legal or illegal. Therefore caution should be taken when tasking DNS Operators with acting as the arbiters of permissible content on the internet.

Registries and Registrars are very diverse in terms of size, activities and governance structures. Moreover, the fundamental distinction between generic and country-code Top Level Domains (gTLDs and ccTLDs) in terms of relation with national laws and authorities, leads to very different approaches and constraints when receiving direct requests or orders for action at the DNS level regarding abuses online, particularly when they originate across borders. In the absence of a generally accepted framework regarding how to deal with abuse, DNS Operators' practices vary considerably.

Therefore, defining when it is appropriate to act at the DNS level to address abuses requires communication between all stakeholders to help them understand each other's situation, concerns and intentions; agreed norms of behavior to foster informal or structured coordination; and processes to develop practical cooperation mechanisms.

The Domains & Jurisdiction Program Contact Group, consisting of experts from governments, internet companies, technical operators, civil society, leading universities and international organizations has, over the years, identified the key issues that could structure new models of transnational cross-border action to address DNS abuses.

A common objective of the different actors should be the definition of high substantive and procedural standards regarding:

- Under what strict conditions might interruption of a domain name without consent of the registrant be envisaged/acceptable;
- What actions should/would domain name operators be willing and able to exercise;
- What rules and procedures could help establish or enhance the credibility of notifiers' notifications (for information or action); and
- What possible mechanisms can help improve transparency in such processes?

2. I&JPN METHODOLOGY

The Internet & Jurisdiction Policy Network fosters a new approach to transnational policy-making. Its innovative methodology identifies relevant stakeholders to define common problems and produce solutions to pressing and complex policy challenges. The neutral and replicable approach, structures interactions among diverse policy actors who would normally not have the opportunity to work together on practical and concrete outcomes.

Since 2016 in regular iterations, the Domains & Jurisdiction Program Contact Group engages a selected set of these global policy actors while trying to ensure balanced geographical representation from governments, internet companies, technical operators, civil society, leading universities and international organizations. Using the I&JPN Methodology, Contact Groups have iteratively developed concrete outcomes pertaining to specific facets of DNS-level action to address abuses. Based on this methodology, future Contact Groups will continue to develop specific policy outcomes on focused issues while also addressing emerging challenges.

Meet the Members of the Domains and Jurisdiction Contact Group from 2018 - 2020 here.

The Internet & Jurisdiction Policy Network fosters a new approach to transnational policy-making. Its innovative methodology identifies relevant stakeholders to define common problems and produce solutions to pressing and complex policy challenges.

FRAMING COMMON PROBLEMS

Issues can best be addressed when formulated as problems that stakeholders have in common rather than with one another. As a first step, stakeholders are consulted to develop a shared framing of the issue at hand and build a shared vernacular. This helps develop a common understanding of the policy problem and helps identify key areas for cooperation where stakeholders can work collaboratively to develop practical and operational solutions.

How can the neutrality of the internet's technical layer be preserved when national laws are applied to the Domain Name System?

I&JPN Domains & Jurisdiction Framing Paper (2017)[i]

SETTING COMMON OBJECTIVES

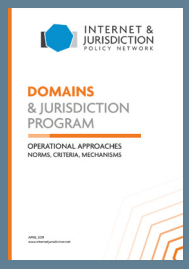
Based on these areas of cooperation, a dedicated Contact Group, guided by a neutral and independent coordinator, identifies key structuring questions that guide discussions among stakeholders and provide a framework within which concrete policy solutions can be developed. These discussions documented as Policy Options define common objectives to ensure better policy coherence and structure further work.

This document aims at providing, in a forward-looking approach, guiding elements to structure further discussion on possible frameworks regarding cross-border DNS-level action to address abuses. It explores the due process dimensions of voluntary regimes envisaged by some DNS operators to deal with domain takedown requests and the potential role of so-called "notifiers".

I&JPN Domains & Jurisdiction Policy Options (2018)[ii]

DEVELOPING COMMON APPROACHES

Based on the objectives identified, intense work in the Contact Group aims to develop scalable, interoperable policy solutions. These can take the form of Operational Norms – to help actors organize their own behavior and mutual interactions; Operational Criteria – to guide actors who develop, evaluate & implement solutions; and Operational Mechanisms – which offer concrete avenues for cooperation.



The work of the dedicated Contact Group of the Internet & Jurisdiction Policy Network aims to contribute to policy discussion by addressing key elements of cross-border DNS-level action to address abuses.

I&JPN Domains & Jurisdiction Operational Approaches (2019)[iii]

FOSTERING LEGAL INTEROPERABILITY

Further work is conducted to evangelize, communicate and aid the implementation of these policy solutions. This may take the form of Toolkits compiling thematic Outcomes developed by the Contact Group. This helps further legal interoperability in two dimensions:

- **Interoperability between actors**: to enable automation of the technical workflow among public authorities and private actors across borders to ensure due process at scale.
- **Interoperability between norms**: to reduce the potential of conflicts in rule-setting, implementation and enforcement among different regimes.

i. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Paper.pdf
ii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Policy-Options-Document.pdf
iii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

The DNS Level Action to Address Abuses Toolkit frames approaches towards defining thresholds of when action at the DNS level is appropriate and builds a common understanding of the requisite processes that can ensure due process. This resource can be useful for DNS Operators in the design of their DNS Abuse related activities, and for Notifiers in the detection and reporting of problematic activity within the DNS. It can also help legislators and policymakers determine procedures for dealing with different types of DNS Abuse. This Toolkit provides tools that seek to help improve the interactions between the different actors to act on DNS Abuse while also strengthening corresponding procedures and mechanisms to guarantee proportionate remedies and due process for registrants. The Domains & Jurisdiction Contact Group will continue to engage on the topics addressed in the Toolkit with the objective of refining them and developing new tools.

The subsequent components of this Toolkit are a joint contribution by some of the most engaged experts in this field to advance the ongoing debate on the complex issues of cross-border domain name suspensions. They should not be however understood as the result of a formal negotiation validated by these Members' organizations. They are a best effort by the Members of the Program's Contact Group to address the important cross-border issues pertaining to addressing abuses at the DNS level that have been curated by the I&JPN Secretariat into the framework of this Toolkit.

This Toolkit provides resources that seek to help improve the interactions between the different actors to act on DNS Abuse while also strengthening corresponding procedures and mechanisms to guarantee proportionate remedies and due process for registrants.

3.
TOOLKIT
DNS LEVEL ACTION TO ADDRESS ABUSES

STRUCTURE

ADDRESSING ABUSE AT DNS LEVEL (GENERAL)

ADDRESSING TECHNICAL ABUSE

STRUCTURE

The following Toolkit curates tools that practitioners can use in their everyday work to determine when - and how - it is appropriate to act at the DNS level to address abuses. These tools have been developed by the multistakeholder Domains & Jurisdiction Program Contact Group throughout 2019-20 and also draw on the Operational Approaches document published by the Contact Group in April 2019.

This Toolkit has a twofold structure, each organized along the four stage framework of: identification, evaluation, choice of action, and recourse. The first section 'Addressing Abuse At DNS Level' provides a set of generic tools that shape actors' overall understanding of the types of abuses for which operators receive requests to act on, and actions available to DNS Operators, as well as the effects and implications of such actions. The second section 'Addressing Technical Abuse' contains practical tools specifically targeting technical abuse. This section also contains a Procedural Workflow outlining the process and specific points of interaction between actors in addressing phishing and malware abuse.

ADDRESSING ABUSE AT DNS LEVEL (GENERAL)

IDENTIFICATION

- TYPES OF ABUSES
- DUE DILIGENCE BY NOTIFIERS
- NOTIFICATION TO REGISTRANTS

EVALUATION

- THRESHOLDS

CHOICE OF ACTION

- TYPES OF ACTIONS
- EFFECTS OF ACTION AT THE DNS LEVEL

RECOURSE

- RECOURSE FOR REGISTRANTS
- TRANSPARENCY

ADDRESSING TECHNICAL ABUSE

IDENTIFICATION AND NOTIFICATION OF TECHNICAL ABUSE

- CHANNELS/SOURCES/TYPOLOGY OF TECHNICAL ABUSE NOTIFIERS
- DNS-LEVEL ACTION TO ADDRESS TECHNICAL ABUSES: DUE-DILIGENCE GUIDE FOR NOTIFIERS
- MINIMUM COMPONENTS FOR TECHNICAL ABUSE NOTICES

EVALUATION OF TECHNICAL ABUSE

- DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

ACTING ON TECHNICAL ABUSE

- DNS TECHNICAL ABUSE: CHOICE OF ACTION

PROCEDURAL WORKFLOW

- ADDRESSING PHISHING AND MALWARE

ADDRESSING ABUSE AT THE DNS LEVEL (GENERAL)

IDENTIFICATION AND NOTIFICATION

EVALUATION

CHOICE OF ACTION

RECOURSE

IDENTIFICATION AND NOTIFICATION

Addressing DNS Abuse begins with the identification of abuse that meets a sufficient threshold to justify action at the DNS level. The tools in this section respectively address:

- The types of abuses for which DNS Operators receive requests to act upon.
- The requisite due diligence by Notifiers in the identification of such abuse.
- The modalities of notification to Registrants when it is deemed appropriate to act on specific domains engaged in abuse.

I&JPN Ref. 19-126

TYPES OF ABUSES

DNS Operators receive cross-border requests to take action against domain names allegedly associated with technical abuse or problematic content. Listed below are descriptions of different types of technical abuses, as well as website content abuse, for which Registries and Registrars often receive such requests.[1]

1. Technical abuses

Domain names can be misused to propagate different types of technical abuse, including but not limited to the following:

a. **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.[2]

b. **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or "look-alike" emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.

c. **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to their own site instead of the one initially requested. DNS poisoning causes a DNS server to respond with a false IP address bearing malicious code.[3] Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

d. **Botnets** are collections of internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.[4]

e. **Fast-flux** hosting is used to disguise the location of websites or other internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use the DNS to frequently change the location on the internet to which the domain name of an internet host or name server resolves.[5]

---

1. These lists are illustrative and not intended to be exhaustive.
2. See M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), at https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety-Net_Brochure-web2-2015-06.pdf; "Malware" page at the U.S. Federal Trade Commission website, at https://www.consumer.ftc.gov/articles/0011-malware
3. See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://thenew.org/org-people/about-pir/policies/org-idn-policies/anti-abuse-policy-org-idn/; entries for DNS hijacking and DNS poisoning in the Kaspersky Lab Encyclopedia, at https://encyclopedia.kaspersky.com/glossary/dns-hijacking/
4. See "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, at: https://niccs.us-cert.gov/about-niccs/glossary#B
5. See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://thenew.org/org-people/about-pir/policies/org-idn-policies/anti-abuse-policy-org-idn/

f. **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.[6] Spam is included here to address when it is used as a delivery mechanism for technical abuse.

2. Website content abuses

Most DNS Operators treat requests to deal with problematic website content differently from technical abuses. Since Registries and Registrars (when not also serving as the hosting provider) cannot remove offending pieces of content from a website, more often than not, acting at the DNS level is not appropriate. Remediation for problematic content should occur at the registrant or hosting provider level.

The descriptions below are derived from various sources, including input from I&JPN Contact Group members. They are neither offered nor intended to be interpreted as normative descriptions. Some types of problematic content find a higher degree of shared agreement across jurisdictions than others.

a. **Child abuse material** consists of photos or videos taken by an offender, documenting the sexual abuse of a child.[7]

b. **Controlled substances and Regulated goods** for sale or trade, include illegal drugs, the illegal sale of legal drugs, illegal services, stolen goods, and illegal firearms or other weapons. The legality of a given substance or good will vary across jurisdictions.

c. **Violent extremist content** includes content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.

d. **Hate speech** includes advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[8]

e. **Intellectual property** related domain name suspension requests in response to website content (not relating to the domain name itself) have been issued on the basis of alleged trademark (e.g. sale of counterfeit goods), patent or trade secret infringement, or piracy of copyrighted works. As with all categories above, laws regarding intellectual property differ across jurisdictions.

6. See "The Definition of Spam" by The Spamhaus Project, at https://www.spamhaus.org/consumer/definition/
7. Interpol, "Online child abuse material: Q & A" (January 2017). https://www.interpol.int/Media/Files/Crime-areas/Crimes- against-children/Online-Child-Abuse-%E2%80%93-Questions-and-Answers
8. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS171 (ICCPR), Art. 20(2), at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

I&JPN REF. 19-130

DUE DILIGENCE BY NOTIFIERS

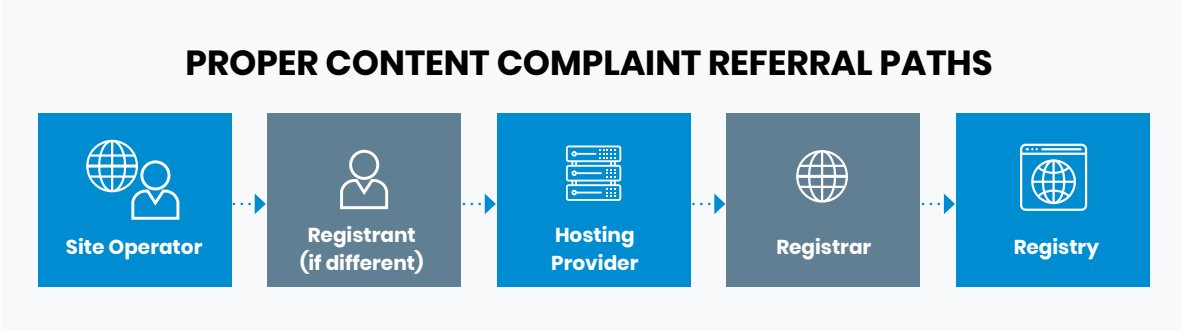
1. General principle

Persons or entities that file complaints or make abuse notices (notifiers) to domain name Registrars and Registries should ensure that they have conducted proper due diligence (both substantive and procedural) prior to alleging a domain name is engaged in abuse, either DNS/technical abuse (security and stability abuses) or in the context of content complaints (website content abuses).

2. Operational considerations

a. Substantive due diligence
Substantive due diligence involves ensuring that any claim against the content of any domain is properly investigated, substantiated and documented (e.g. screen shots, listing on any blacklists, evidence of ownership in claims of infringement). A notifier should ensure that it has undertaken proper substantive due diligence before making a referral.

b. Procedural due diligence
Procedural due diligence involves a hierarchy (see Proper Content Complaint Referral Paths below) of where the notice should be made. For technical abuse, notices directly to the Registrar and Registry are appropriate. In instances of content complaints, mitigation at the DNS level is an imperfect remedy. Accordingly, notices should be made in the following order:



Currently, some notifiers for content complaints make their referrals directly to the Registry or Registrar. This can lead to problems with proportionality.

i. Using the example of a file sharing site, if a Registrar or Registry suspends the entire domain because of an allegation regarding a limited number of infringing or offensive content, then potentially thousands of other pieces of legitimate content are rendered inaccessible by not just the registrant, but end users.

ii. The website operator, registrant or hosting provider, however, can all affect and likely remove the limited instances of abusive content while leaving the remaining content (as well as the domain name) unaffected.

Accordingly, for content complaints, a notifier should first attempt to work with the website operator, the registrant and the hosting provider to have the specific pieces of content removed. If none of those actors ultimately act or remove the content, the notifier may wish to escalate to the Registrar or Registry (such referral would still be subject to applicability of any Acceptable Use or similar policy).

I&JPN REF. 19-133

NOTIFICATION TO REGISTRANTS

1. General principle

Registrants should generally be provided with notifications of alleged abuse before a Registrar or Registry acts against a domain name. There are, however, some allegations of abuse where this is not practical, advisable, or even permissible, and in those instances, notification after the fact should be provided, unless legally forbidden.

2. Operational considerations

a. Registrant notification before action

If a Registry or Registrar receives allegations of copyright infringement, allegations of defamation, instances where content may be inferred to be illegal or fraudulent but cannot be proven without further investigation[9] (generally, "content complaints"), notification to the registrant should occur prior to a DNS Operator taking action on the domain.

b. Registrant notification after action

If a Registry or Registrar receives allegations of DNS technical abuse ("technical abuse"), court orders from competent jurisdiction(s) directing action or as set forth in applicable Registrar or Registry policies or procedures, notification to the registrant can occur after the fact.[10]

c. Who provides the notification?

Between the Registrar and Registry, Registrars are the preferred operator to provide notifications to registrants. Registrars usually have a closer contractual and business relationship with the registrant, and the Registrar collects the registrant's information. Many ccTLD Registries have direct contractual or business relationships with the registrant and may be similarly positioned to provide notifications.

gTLD Registries typically (but not always) provide notifications to Registrars who are asked to work with the registrant to remediate the alleged abuse. In non-court-mandated situations, abuse notifications are usually sent to the Registrar who is then requested to work with the registrant in a limited time frame (e.g. 48 hours) to remediate the alleged abuse.

d. Content of the notice

In most cases, only information necessary to inform the registrant's investigation and remediation of the alleged abuse should be provided in a notification. In some instances, the entire referral may be transmitted (e.g. in instances of alleged copyright infringement if that is in scope of the relevant parties' terms).

---

9. This assumes the various categories of content fall within the scope of the Registry or Registrar's Terms of Service, Anti-Abuse or Acceptable Use Policies or other governing terms. If the content falls outside the scope of such terms, no Notification will be typically provided and the domain will not be actioned.

10. There are also instances when a DNS Operator cannot provide Notification at all (such as when a court order requires confidential handling, or after weighing relevant law enforcement considerations).

EVALUATION

Once potential abuse has been identified in connection with a specific domain name, the next step is an in-depth evaluation towards making a decision on whether the abuse meets a sufficient threshold justifying taking action at the DNS level. This part of the Toolkit sets out the criteria that should be considered.

I&JPN REF. 19-127

THRESHOLDS

1. Technical abuse

Acting at the DNS level is generally justified in situations of technical abuse in order to protect the stability and security of the global infrastructure of the internet. Specific additional measures are nonetheless justified to assist the registrant if the domain is obviously compromised by third parties without his/her knowledge.

2. Abusive content

Given the geographically global impact of an action at the DNS level, doing so regarding abusive content can only be justified if a particularly high threshold of abuse/harm is met, regarding *inter alia*:

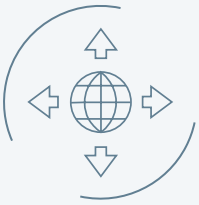
a. The degree of global normative coherence[11] regarding the alleged abuse: i.e. whether the content at issue is considered illegal across a sufficient number of jurisdictions;

b. The proportion of the site effectively dedicated to the infringing content;

c. The manifest intended purpose or bad faith of the registrant, and

d. The lack of available alternative measures to remediate the situation.

11. See International Normative Coherence in I&J Policy Brief on the Geographic Scope of Content Restrictions: https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-102-Geographic-Scope-Content-Restrictions.pdf



CHOICE OF ACTION

Once a decision to act on a domain name has been made, Operators need to determine the specific action which can be most effective and appropriate to address the abuse. The following section sets out the tools that are available to DNS Operators and their practical effect, to guide the determination of the right course of action:

- A non-exhaustive list of the different types of actions at the disposal of Operators.
- An explanation of the technical effects of such actions.

I&JPN REF. 19-131

TYPES OF ACTIONS

Protection of the core of the internet is and should be a key priority. The DNS - part of the core of the internet - is an addressing system. It is a neutral, technical layer that is vital for the proper functioning of the internet. Action at the DNS level is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content.

Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is important that the impact of a specific action at DNS level is well understood.

Requests for domain name suspension should be directed in the first instance to those parties that are closest to the abusive activity, including by contractual relationship (see Proper Content Complaint Referral Paths under 'Due Diligence by Notifiers' for more detail). For example, notifiers should first attempt to contact the domain name registrant, and then the hosting provider (either or both of which may be the wrongdoer), as these parties have the most direct relationship to the website content.[12] Direct action by registrants or hosting providers minimizes potential impact on the functioning of the DNS. If these attempts are unsuccessful, notifiers should consider the below options. Listed below are different types of actions that Registries and Registrars may take, as appropriate, in response to cross-border suspension requests.[13]

Note that the availability of any given action below may vary across providers.

1. For Registries: **Refer the suspension request to the Registrar**, which has the contractual relationship with the Registrant of the domain name.
2. **Hold** the domain name so it does not resolve. This removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public Internet. In the event that the request was made in error, this action may be reversed.
3. **Lock** the domain name so it cannot be changed. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve.
4. **Redirect** name services for the domain name. A Registry has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected for "sink-holing" (logging traffic) to identify victims for the purposes of remediation.
5. **Transfer** of the domain name to a suitably-qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.
6. **Delete** the domain name. Deletion is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. Restoring a domain name, if the deletion is found to be inappropriate, may involve additional burdens that are not manifest when placing a domain name on hold. Deletion is generally not as effective at mitigating abuses as suspension, as a registrant is free to re-register the domain name after it is purged from the zone.

---

12. See CENTR, Domain name registries and online content (Jan 30, 2019), available at: https://centr.org/library/library/policy-document/domain-name-registries-and-online-content.html (describing the relationships between various actors involved with a website featuring abusive content).

13 . These actions are adapted from ICANN's Framework for Registry Operator to Respond to Security Threats, at https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en (Internal citations omitted).

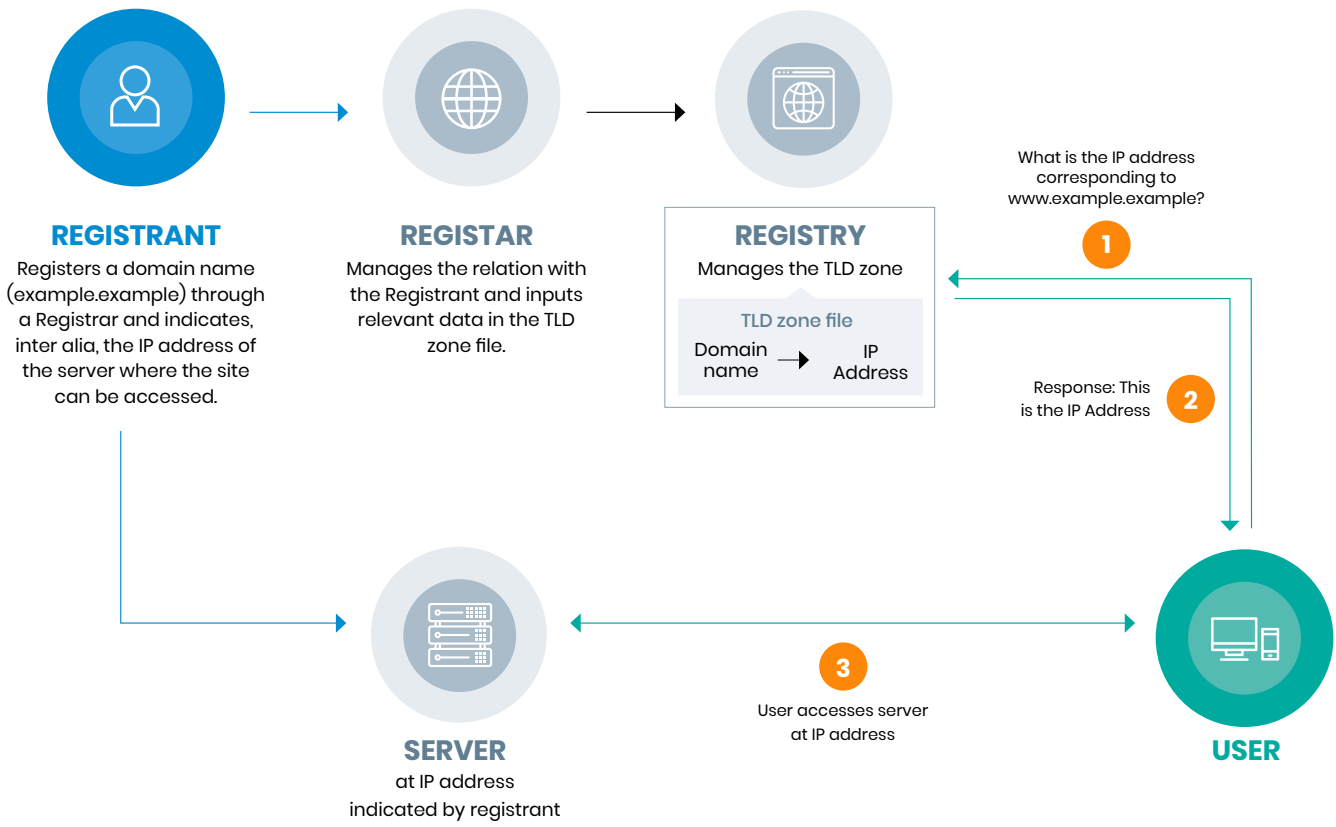
I&JPN REF. 20-101

EFFECTS OF ACTIONS AT THE DNS LEVEL

Action at the DNS level is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content. Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm can potentially justify resorting to such a measure.

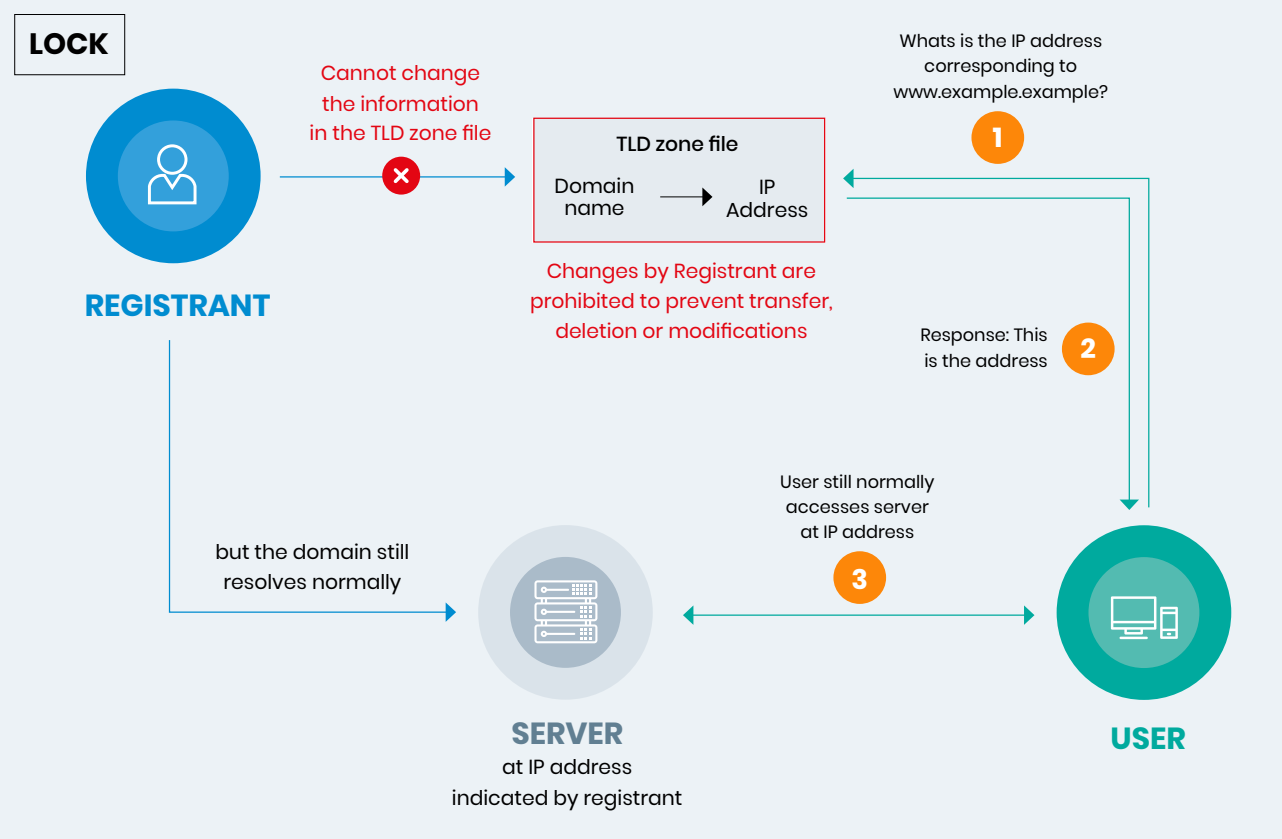
In any case, requests for action should be directed first to parties that are closest to the abusive activity, including by contractual relationship, in order to minimize impact on the functioning of the DNS. If attempts to reach the registrant or the hosting provider are unsuccessful, notifiers should consider the different types of actions listed below that Registries (who manage the Top Level Domains ("TLDs")) and Registrars may take, as appropriate, in response to cross-border suspension requests. It is important that the functioning of the DNS and the impact of each specific action at DNS level are well understood.

The basic functioning of the Domain Name System

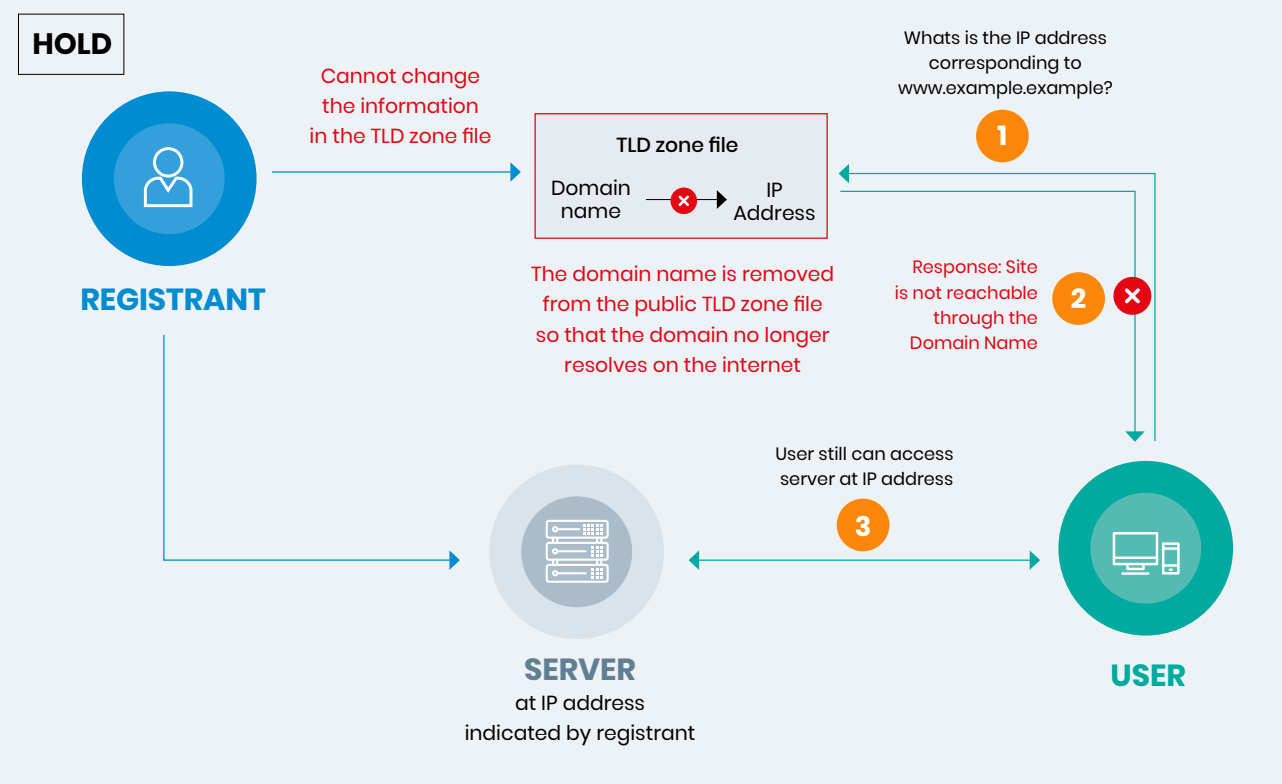


ACTIONS

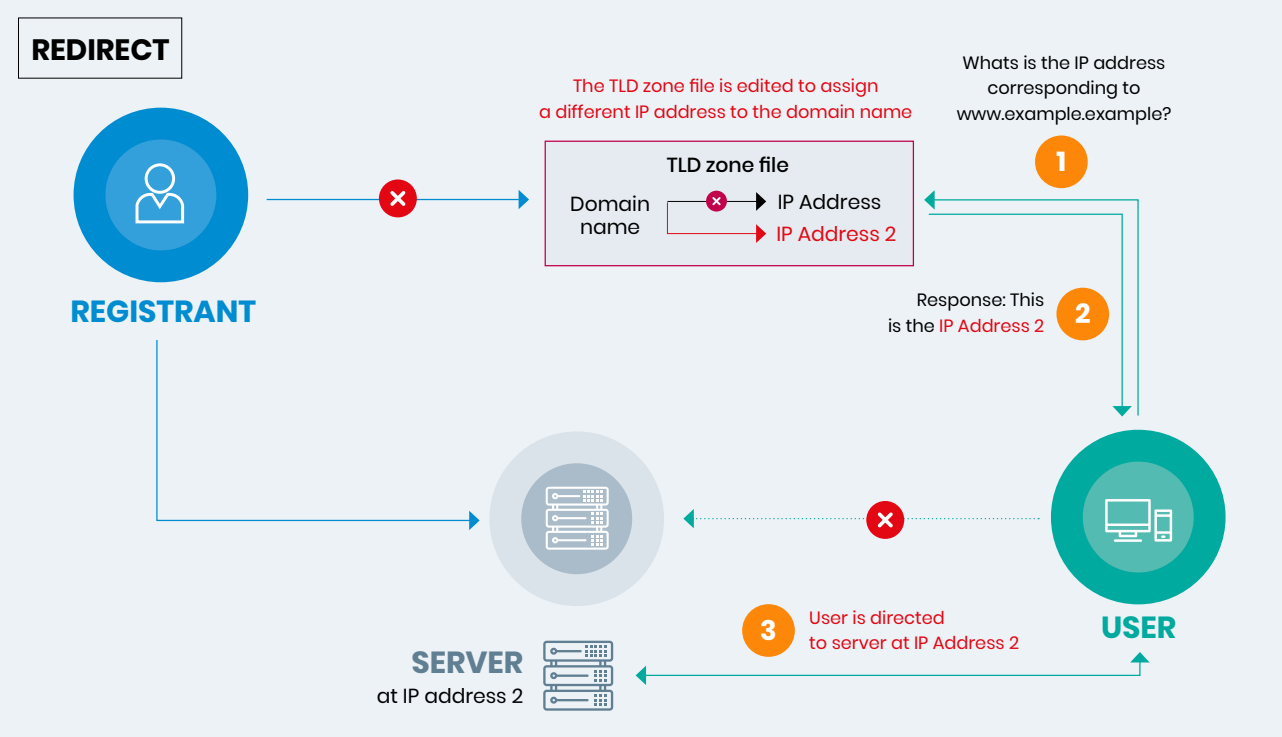
ACTION 1: LOCK A locked domain cannot be transferred, deleted or have its details modified, but still resolves.



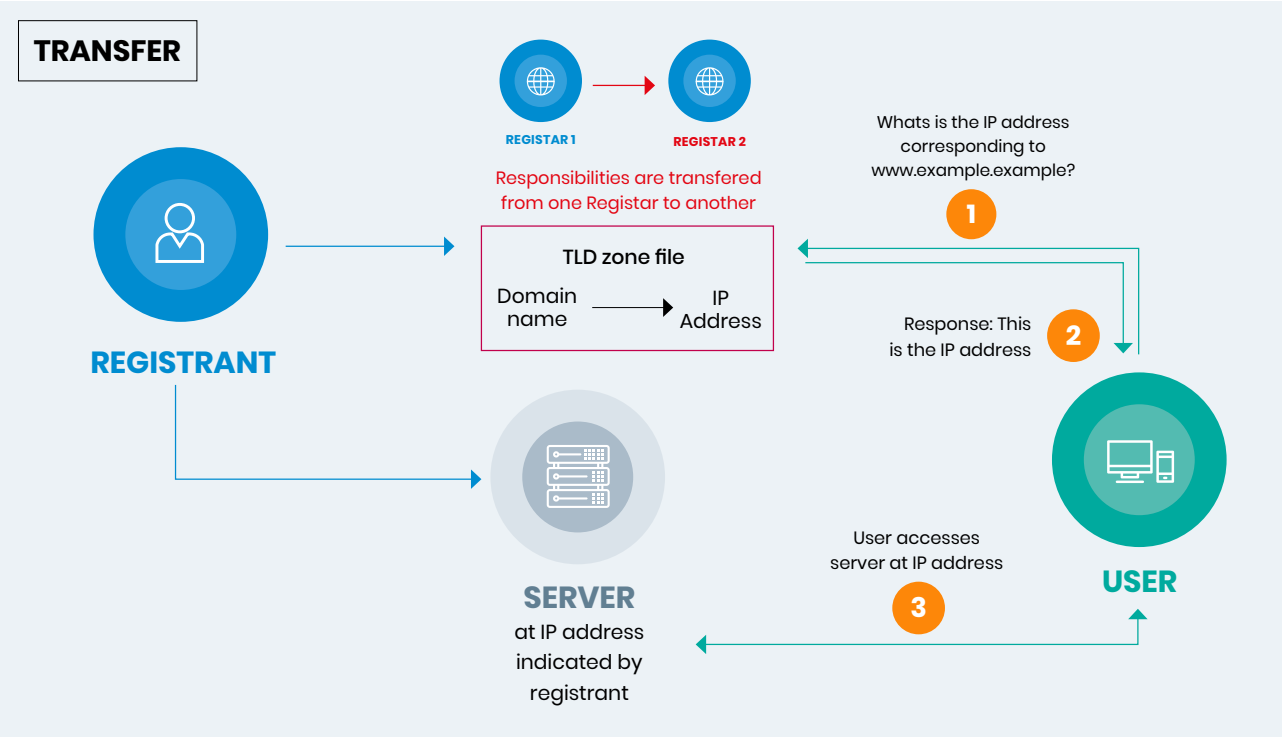
ACTION 2: HOLD This action removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public Internet. In the event that the request was made in error, this action may be reversed. Importantly, the site still remains accessible through the IP address.



ACTION 3: REDIRECT By changing the nameservers for the domain name, associated services can be redirected without consent of the registrant, for instance for "sink-holing" (logging traffic) to identify victims for the purposes of remediation. This measure is usually done in conjunction with 'Lock', and the registrant is typically not informed of the action in advance.



ACTION 4: TRANSFER Transfer of the domain name to a qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.



ACTION 5: DELETION Deleting a domain name is an extreme action and **not generally recommended** without careful due diligence. Restoring the domain name would involve additional burdens absent when placing a domain name on hold. More importantly, **registrants are free to re-register the domain** name after it is purged from the zone.

RECOURSE

Recourse is an essential part of due process. It is independent from the evaluation conducted ahead of the action being taken by Operators on a domain name and must provide avenues for registrants to challenge such action and obtain redress. This section outlines the following tools:

- Principles to structure mechanisms for registrant recourse.
- A two-dimensional approach to foster transparency.

I&JPN REF. 19-134

RECOURSE FOR REGISTRANTS

1. General principles

Registrars and Registries should maintain a publicly available process (even an informal one) for allowing a registrant to contest or appeal an action against a domain name for technical abuse or for a content complaint. Any appeal must include independently verifiable evidence that does not require (or at least minimizes the need for) the DNS Operator to interpret the law, which is generally outside the DNS Operator's expertise.

2. Operational considerations

a. Process

Registries and Registrars should note in their Anti-Abuse Policy/Acceptable Use Policy how such an appeal can be lodged.

i. This will typically be something along the lines of "For inquiries regarding actions taken pursuant to this policy, please contact [abuse@example.example or review@example.example]"

This process will be available for actions except those carried out pursuant to a court order from the DNS Operator's jurisdiction. If action was taken pursuant to an order from a court with jurisdiction over the DNS Operator, no internal DNS Operator process can overrule such an order. The DNS Operator should conduct proper and thorough due diligence before action on the domain is effectuated. This should obviate the need for much back-and-forth with the registrant on appeal.

b. Evidence submitted

Registries and Registrars are not courts of competent jurisdiction, nor are they experts in interpreting various applicable laws. Accordingly, any evidence submitted by a registrant/appellant must be independently verifiable and not require (or at least minimize the necessity for) the DNS Operator to interpret the law. For a DNS Operator to reverse its decision in such an appeal, the evidence must be overwhelming and objective. It is important to have such a mechanism in case, for instance, of DNS Operator error or overwhelming evidence provided against the notifier's complaint.

c. Overturning action regarding technical abuse

There is less "wiggle room" in evaluating technical abuse than in evaluating abusive content. If a domain was engaged in phishing or distribution of malware and identified as such, only evidence clearing a high threshold should allow for reversal of a suspension, unless the domain has been compromised.

i. If a registrant is able to show the domain was compromised without his/her knowledge, the DNS Operator may wish to consider such evidence.

ii. Another instance for a DNS Operator to reverse a decision for technical abuse would be for DNS Operator error, such as suspending the wrong domain name (example1.example instead of example11.example), or if a domain was removed from a blocklist that was relied upon prior to suspension.

d. Overturning action regarding website content abuse

There is more room for interpretation here by a DNS Operator for content complaints, but any evidence submitted must be independently verifiable and not require, or at least minimize the necessity for, the DNS Operator to interpret the law.

If a registrant appeals an action a DNS Operator took due to reliance on work with a third party (such as a specialized notifier), the DNS Operator and notifier should have a process in place whereby the notifier can independently assess the countervailing evidence and be willing to reverse its recommendation.

I&JPN REF. 19-132

TRANSPARENCY

A two-dimensional approach can help to improve transparency:

1. Statistics

Beyond metrics currently used for performance measurement, DNS Operators are encouraged to develop metrics for collecting and reporting, in exportable, and accessible formats, coherent statistics pertaining to abuse notifications and implemented actions. Public authorities and specialized notifiers should likewise develop corresponding mechanisms to ensure traceability of their notices.

2. Decision-making

DNS Operators document and make available to the public the criteria determining when action at the DNS level is appropriate, the types of abusive content they are willing to take action on, and their abuse point(s) of contact. They also document and publicize their internal criteria for decision-making and the channels for appeals/recourse. Specialized notifiers likewise document and make available to the public their criteria for evaluation of abuses, as well as their due diligence rules and procedural guarantees.

ADDRESSING TECHNICAL ABUSE

IDENTIFICATION AND NOTIFICATION OF TECHNICAL ABUSE

This section of the Toolkit lays out practical tools that can help different third-parties (Notifiers) in their identification and notification of technical abuse, including:

- A typology of the sources that provide notifications on technical abuses to DNS Operators, referred to herein as “Notifiers”;
- The requisite due-diligence expected from such Notifiers in the notification of technical abuse; and
- The minimum notice components that must be included in the notification of such technical abuse.

I&JPN REF: 20-110

CHANNELS / SOURCES / TYPOLOGY OF TECHNICAL ABUSE NOTIFIERS

DNS Operators receive technical abuse complaints ("Notices") from a variety of sources representing different types of stakeholders in the DNS ecosystem ("Notifiers"). Whether and how DNS Operators take action in response to Notices depends on many factors, including, but not limited to whether the Notice contains information required for evaluation and possible action by the Operator, whether the Operator has a pre-existing relationship (contractual or otherwise) with the Notifier concerning detection and remediation of the type of abuse alleged[14], the Operator's contractual obligations to third parties (e.g. ICANN), the Operator's Terms of Service and the local jurisdictional framework. In all cases, Notifiers should exercise careful due diligence before requesting Operators to take action at the DNS Level to address alleged abuses.

The table below provides an overview of the types of notifiers, as well as examples of entities or persons that fall within each given type. Such examples are not meant to be exhaustive nor prescriptive. Some categories of notifiers may fall within more than one type: for example, a Reputation Block List Provider may be a non-commercial entity. Likewise, a DNS Infrastructure Provider may be a commercial or non-commercial entity.

TYPES	NOTIFIERS
Individuals	DNS users acting in their personal capacity
Governments (Domestic, Regional, Foreign)	Court orders
	Public Administration Bodies (e.g. Regulators, Public Safety Administrators, CSIRTs)
	Law enforcement
DNS Infrastructure Providers	Registries Registrars and resellers Back-end service providers Technical solutions and security providers ICANN
Commercial Entities	Reputation blocklist providers CERTs Businesses and consultants
Non-commercial entities	Mission-based organizations that are dedicated to furthering the public interest
Machine	Artificial Intelligence

14. Operators may enter into contractual obligations with different notifying entities. According to the terms of such agreements, the DNS Operator can determine the level of evaluation that it may undertake.

I&JPN REF: 20-113

DNS-LEVEL ACTION TO ADDRESS TECHNICAL ABUSES: DUE-DILIGENCE GUIDE FOR NOTIFIERS

All notifiers have a duty to conduct due diligence before making notifications of alleged technical abuse[15] to DNS Operators and requesting action at the DNS level to remedy such abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged. By employing *procedural and substantive*[16] due diligence measures before making notifications to the DNS Operator, notifiers can increase the efficiency and effectiveness with which the Operator evaluates and addresses notifications of alleged abuse.

This document lists a series of questions notifiers should ask themselves in order to determine that making notices to operators is appropriate. This guide is structured around three parts: Identification; Evaluation; and Notification. The Identification and Evaluation sections list the *substantive* due diligence a notifier is encouraged to perform to determine that abuse is present and whether action at the DNS level is appropriate to address it. The Notification section indicates the level of *procedural* due diligence that notifiers are encouraged to conduct in order to ensure that the notice is addressed efficiently and effectively.

IDENTIFICATION

The following questions will help notifiers when identifying potential abuse:

- What triggered the Notifier's attention to this abuse and does the Notifier have first-hand knowledge of the alleged abuse?
- What is the type of technical abuse at stake? Does this appear to be something that can and should be mitigated at the DNS level?
- What is the evidence for the existence of such alleged abuse?
- Is it likely that the domain has been compromised, i.e. the infringing action has been done without the knowledge or intent of the registrant/site operator?

EVALUATION

When making a referral to a DNS Operator or Infrastructure Provider, notifiers should make the referral to the entity closest to the abuse and most likely to be able to evaluate the specific problem and remediate it with the least collateral damage. The questions below can help a Notifier determine which Operator is best positioned to help:

---

15. For scope of technical abuse, refer to 'Types of Abuses' in the Addressing Abuse at DNS Level (General) part of this toolkit.

16. Refer to Criteria E2: Due Diligence by Notifiers in Domains & Jurisdiction Operational Approaches

- Where is the abuse taking place (e.g. sublevel domain, specific URL, etc.)?
- Is action at the DNS[17] level appropriate or are there other means to address the abuse?
- If there is a more appropriate actor than a DNS Operator to address the abuse (e.g. hosting provider or site operator), has there been an attempt to address the abuse at that level?
- Would action at the DNS level create collateral damage disproportionate to the harm caused by the alleged abuse?
- What could be the appropriate choice of action at the DNS level to address the abuse?
- Who are the relevant registry and registrar and how do their respective terms of service address such type of abuse?
- Is there a way to assess (including through interaction with relevant authorities) if there is an ongoing investigation that a DNS-level action could jeopardize?

NOTIFICATION

When making notification to DNS Operators, Notifiers should consider the following questions to improve the efficiency and efficacy of their notices:

- When action at the DNS level is appropriate, to whom should notification be made: Registrar, Registry, both?
- Does the notifier have an existing contractual relationship with the Operator and have the terms of such a contract been met?
- What is the DNS Operator's preferred channel for notification of abuse?
- Does the DNS Operator have a prescribed reporting format?
- Does the notice contain all the required components for a good/effective notice[18]?
- Should the notice be designated confidential, e.g. in cases where there is a risk of jeopardizing an investigation?

17. Refer to I&J Educational Resource on Effects of Action at the DNS Level

18. Refer to Domains & Jurisdiction Program Outcome Minimum Notice Components for Technical Abuse

I&JPN REF: 20-106

MINIMUM COMPONENTS FOR TECHNICAL ABUSE NOTICES

DNS Operators frequently receive complaints of technical abuse "Notices" in a broad diversity of formats that often do not contain sufficient information for investigation and action. The following table, based on Criteria C of the Internet & Jurisdiction Policy Network Domains & Jurisdiction Operational Approaches document, therefore proposes a list of components that support actionable Notices for reporting technical abuse.[19] While the table indicates a subset of components that are necessary to make a given Notice actionable, as well as those components which significantly assist the operator in addressing the alleged abuse, *all* components listed are important contributions to robust and effective Notices. In general, more detailed Notices are better in assisting the operator's evaluation and response. Additionally, where the notifier submits evidence of alleged technical abuse in the form of attachments (*e.g.* screenshots of alleged phishing), operators may reasonably employ an added layer of security review to ensure that attachments are not infected. This may increase the timeframe for the operator's review of the Notice, depending upon the operator's internal security capabilities.

Elements marked with a red asterix(*) are components without which Notice is not actionable. Those highlighted in blue can significantly help the operator deal with the Notice.

IDENTIFICATION		Components without which notice is not actionable (A)
Time*	Date and time corresponding to the issuance of the request.	A
Type of Notifier	Refer to Typology of Notifiers (court, law enforcement, private notifier, legal representative of a complainant, Anonymous)	
Issuing Entity[20]*	Identification of the requester	A
Request ID number	Reference provided by the issuer of the request (if applicable).	
Registrar (if Notice is addressed to the Registry)	Name and Abuse Point Of Contact of the Registrar managing the registration.	
Registry (if the Notice is addressed to the Registrar)	Registry managing the corresponding TLD extension. If not known, indicate the TLD.	
CASE – In case of court order from court of applicable jurisdiction		
Type of abuse*	Indication of the type of abuse alleged (from taxonomy list)	A
Legal basis*	A copy of the court order	A

19. The criteria for notifications for Website Content Abuse are considered separately, not in this document.

20. While the identity of the person or entity making the Notice is generally required for operator's to fully evaluate a given Notice, there are circumstances where operators may accept and evaluate Notices that are submitted anonymously, particularly where the subject matter of the alleged abuse is especially sensitive, such as those involving allegations of Child Sexual Abuse Imagery ("CSAM").

DUE DILIGENCE[21] – In case of no court order from court of applicable jurisdiction		
Evaluation	Steps undertaken by the notifier - prior to notification of the DNS Operator - to establish the existence, and extent of the abuse in conformance with the Operators' applicable policies	
Supporting evidence	Factual documentation of the alleged abuse and evaluation. This may be in the form of listings on reputation block lists (RBLs) the operator relies upon or through direct evidence (like screenshots in the case of phishing).	
Foreign Public Authority*	An official notice, documenting the elements above, including, where necessary, effort to domesticate foreign court order, if any.	A
Proportionality	Justification that the alleged abuse meets a sufficient threshold for action at the DNS Level, and also factoring potential collateral damage and the effectiveness of action at the DNS level.	
REQUESTED ACTION		
Targeted domain(s)*	Specific domain name(s) upon which action is requested, including URL.	A
Action sought*	Indication of the specific action requested (see Types of Action under 'Choice of Action')	A (in case of court order from applicable jurisdiction)
TIMING		
Deadline	When the action(s) should be executed (important in particular in case of concerted actions or emergency)	
Time range	Duration of the requested action (if applicable, if action sought is not 'transfer/delete')	
Emergency	Is this action justified by a particular emergency (nature of emergency)	
Rationale emergency*	Explanation of how the requested action will avert or mitigate the emergency	A(If confidentiality is requested)
CONFIDENTIALITY		
Confidentiality	Request not to notify the registrant prior to action or potentially even ex post for a period of time (if applicable)	
Confidentiality timeline*	Requested duration of confidentiality	A(If confidentiality is requested)
Rationale for confidentiality*	Proper justification for confidentiality request and timeline (can be included in the Court Orders)	
AUTHORITY		
Authentication	Information allowing verification of the identity of the Notifier and the authenticity of its Notice	
Certification	Written self-certification by the Notifier of its competence, performance of prior due diligence and accuracy of its statements and that there is no improper motivation or illegitimate purpose for requesting the suspension/cancellation.	
CONTACTS		
Issuing entity	Contact details of the Notifier, to which notification of action (or non-action) should be sent	
SIGNATURE		

21. For technical abuse, all requests made to ccTLD Operators by notifiers other than a court of applicable jurisdiction can be acted upon on a voluntary basis according to Operators' terms of service and national legislation, when applicable.

EVALUATION OF TECHNICAL ABUSE

Once alleged technical DNS abuse has been notified to DNS Operators, they must make a determination on whether to act on it or not. Towards this, the following section provides Operators guidance for their internal evaluation processes.

I&JPN REF: 20-108

DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

Acting at the DNS level can be justified to remediate technical/infrastructure abuse in order to protect the stability and security of the global infrastructure of the internet. DNS operators rely on a variety of internal and external resources to identify, evaluate and take action to remediate technical abuse[22]. While establishing whether a domain is being used to perpetrate technical abuse tends to produce binary results (i.e. the domain is or is not engaged in technical abuse), care should nonetheless be taken to ensure that action at the DNS level to remediate said abuse is appropriate and proportionate.

A general approach to addressing technical abuse may be based upon the following steps:

- Identification or notification of the alleged technical abuse associated with the domain(s)
- Evaluation of scope of abuse
- Determination of the choice of appropriate and proportionate action
- Technical actions to ensure recourse and remediation

The table below lists a set of structuring questions that DNS Operators can use at each step to determine a course of action to address technical abuse on a voluntary basis.

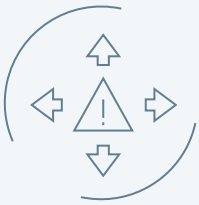
	STRUCTURING QUESTIONS
IDENTIFICATION AND NOTIFICATION	• Is the domain within the DNS Operator's zone? • Does the notice allege technical abuse? • Does the notice contain all the necessary components[23] for identifying abuse and taking action, as appropriate? • Does the notice come from a court of applicable jurisdiction? • Does the notice come from a trusted, repeating or ad-hoc source? • Is there an agreement between the DNS Operator and this specific notifier?
EVALUATION OF ABUSE Multi-factor analysis to evaluate the scope and authenticity of alleged abuse	According to the type of technical abuse, what should DNS Operators take into consideration when evaluating alleged abuse, to ensure that the action taken is appropriate and proportionate? • Conduct own investigation (with help of 3rd parties if required) to determine: - That it is not a false positive - Whether the abuse is still active (hasn't already been mitigated by someone else) - Where the abuse is taking place (single link, single URL, entire site?) • Is it likely that the domain has been compromised, such that the registrant should be contacted? • Is the alleged abuse related to a sublevel or third level domain? • Should action be taken?

22. See 'Types of Abuses' in 'Addressing Abuse At DNS Level' section of this Toolkit

23. Refer to Domains & Jurisdiction Minimum Notice Components for Technical Abuse

CHOICE OF ACTION Choice of the measure used to address the abuse	According to the type and level of technical abuse, what determines the choice of action? • Should the DNS Operator act or should other actors act[24] (e.g. hosting provider)? • If ordered by a court of applicable jurisdiction, is the specified action technically implementable? • What type of action[25] should be taken? • Should the registrant be notified[26]?
RECOURSE AND REMEDIATION Recourse Mechanisms available to registrants	According to each type of technical abuse and type of notice: • When is there notification to the registrant (when applicable)? • What recourse mechanisms[27] are available to the registrant?

24. Refer to Criteria E/2B - Procedural Due Diligence in the Domains & Jurisdiction Operational Approaches
25. Refer to Criteria F - Types of Action in the Domains & Jurisdiction Operational Approaches
26. Refer to Criteria H - Notification to Registrants in the Domains & Jurisdiction Operational Approaches
27. Refer to Criteria I - Recourse for Registrants in the Domains & Jurisdiction Operational Approaches



ACTING ON TECHNICAL ABUSE

This section of the Toolkit provides actors with an understanding of the technical effects of the diverse actions available to DNS Operators and their suitability and effectiveness against specific types of technical abuses.

I&JPN REF: 20-114

DNS TECHNICAL ABUSE: CHOICE OF ACTION

Once technical abuse[28] has been identified, evaluated and confirmed, DNS Operators must decide whether and how to act to address the abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged.

Malware and Phishing are technical abuses that can be delivered through websites or via email (in the form of spam). In such cases, acting on the attendant domain can be used to stop or interrupt its activity within the DNS.

Conversely, pharming, while a form of technical abuse, cannot be remedied through DNS-level action by DNS Operators. Pharming involves the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. These activities do not involve the use of domain name(s) to propagate abuse. Therefore, action at the DNS level is ineffective to address pharming. Signing domains with DNSSEC and enabling validation on resolvers is a systemic approach that can be effective in preventing pharming.

As noted below, the LOCK and HOLD commands are most often used in tandem to address malware and phishing, as, respectively, these commands appropriately prevent the resale or transfer of domains engaged in abuse and remove the domain name from the TLD zone file, thereby preventing the domain from resolving on the public internet. Conversely, as explained below, the Transfer, Redirect and Create commands are of limited use in stopping DNS abuse and are usually implemented by DNS operators only pursuant to formal requests from law enforcement or courts.

The charts below are based on Criteria F 'Types of Action' of the Operational Approaches[29] document and address respectively:

- HOLD and LOCK, most often indicated to remediate technical abuse.
- REDIRECT and TRANSFER, generally used as additional measures upon specific requests.
- DELETE and CREATE, exceptional actions mainly used in the case of botnets and Domain Generation Algorithms (DGA's).

28. For scope of technical abuse, Refer to Annex in Domains & Jurisdiction Program Outcome on DNS Operators' Decision-making Guide To Address Technical Abuse

29. See 'Types of Action' in Addressing Abuse At DNS Level section of this Toolkit

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
LOCK	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	Locking a domain name preserves the *status quo* in terms of ownership, contact information and server configuration. This can assist investigators and fact-finders (*e.g.* courts) in investigating alleged abuse. The *Lock* command also prevents the resale or transfer of domains involved in abuse to unsuspecting third parties. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve through the DNS (i.e. enabling access to the attendant website(s) via the domain name).
HOLD/ SUSPENSION	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	The *Hold or Suspension* command removes the domain name from the TLD zone file and prevents it from resolving on the public internet (i.e. enabling access to the attendant website(s) or other services including emails or 3rd party domains linked via nameservers via the domain name). This helps prevent distribution of malware and exposure to phishing including its distribution via email. The *Hold or Suspension action* is the strongest action applicable to a domain name and can be used to address most technical abuse. It is important to note however, that the attendant website will still remain reachable, albeit only through its IP address.

The actions *Redirect* and *Transfer* ***do not stop or impede ongoing technical abuse***. DNS Operators generally apply these commands only when compelled to do so by a formal request from law enforcement, a court order or other compulsory instruments.

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
REDIRECT	Malware, Phishing, Botnets	A DNS Operator has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected upon request for "sink-holing" (logging traffic), for instance to identify victims for the purposes of remediation.
TRANSFER	Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)	DNS Operators may be compelled to *Transfer* domain names without the registrant's consent in certain limited circumstances, for instance in order to prevent further abuse. This command effects a change in control (administration and ownership rights) of a domain to a third party to prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.

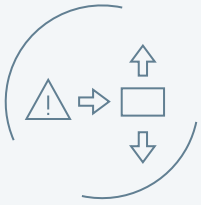
When a domain is deleted, it is removed from the TLD (Top Level Domain) zone file. As a result however, the domain becomes available again to be registered on a first-come, first-served basis.

This may potentially be done by the very registrant[30] who was using the domain to commit abuse. For this reason, the Delete command is generally not widely used to address abuse. The Create command may be also sparingly used for specific forms of technical abuse, such as botnets, but the use of this command raises very important and specific issues[31].

30. In some instances, DNS Operators are required (by court order) to place deleted domain names "on reserve" so that they cannot be re-registered by the perpetrator(s) of abuse. However, DNS Operators who operate pursuant to contractual agreements with ICANN are generally contractually prohibited from placing domains on reserve, except in limited circumstances outside of abuse operators mitigation efforts. Likewise, certain ccTLD (country code Top Level Domains) operators may also be subject to restrictions or prohibition when placing domains on reserve.

31. Criteria F 'Types of Action' in the Domains & Jurisdiction Operational Approaches does not include 'Create', but is included here due to its relevance to the topic. Create has however two important consequences in the ICANN environment: 1) It requires a contractual waiver for DNS Operators and 2) The newly created domains may entail the payment of a recurring fee.

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
DELETE	Botnets	Deleting a domain name is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. The Delete command may assist in interrupting a Botnet by interrupting the command and control path set by the Botnet's controllers. Deletion has a dramatic effect on the domain name holder and related services and cannot be undone in the circumstances when this choice of action is erroneously implemented. However, as noted above, the *Delete* command generally is not as effective at mitigating abuses as other actions such as Hold because the domain(s) can be quickly re-registered by a bad actor.
CREATE	Botnets, Domain Generation Algorithms	DNS Operators are sometimes asked to create and then redirect/ sinkhole domains that are part of a predictive sequence of a Domain Generation Algorithm ("DGA"). DGAs are algorithms seen in various families of malware used to periodically generate a large number of domain names to be used as rendezvous points with their command and control servers. Once created, the actions *Hold, Redirect or Delete* might be used to interfere with the domain names pointing to the servers that form the botnet. In some cases, this may effectively hinder a botnet, as the infected machines require the path provided by the control domain names in order to "call home".



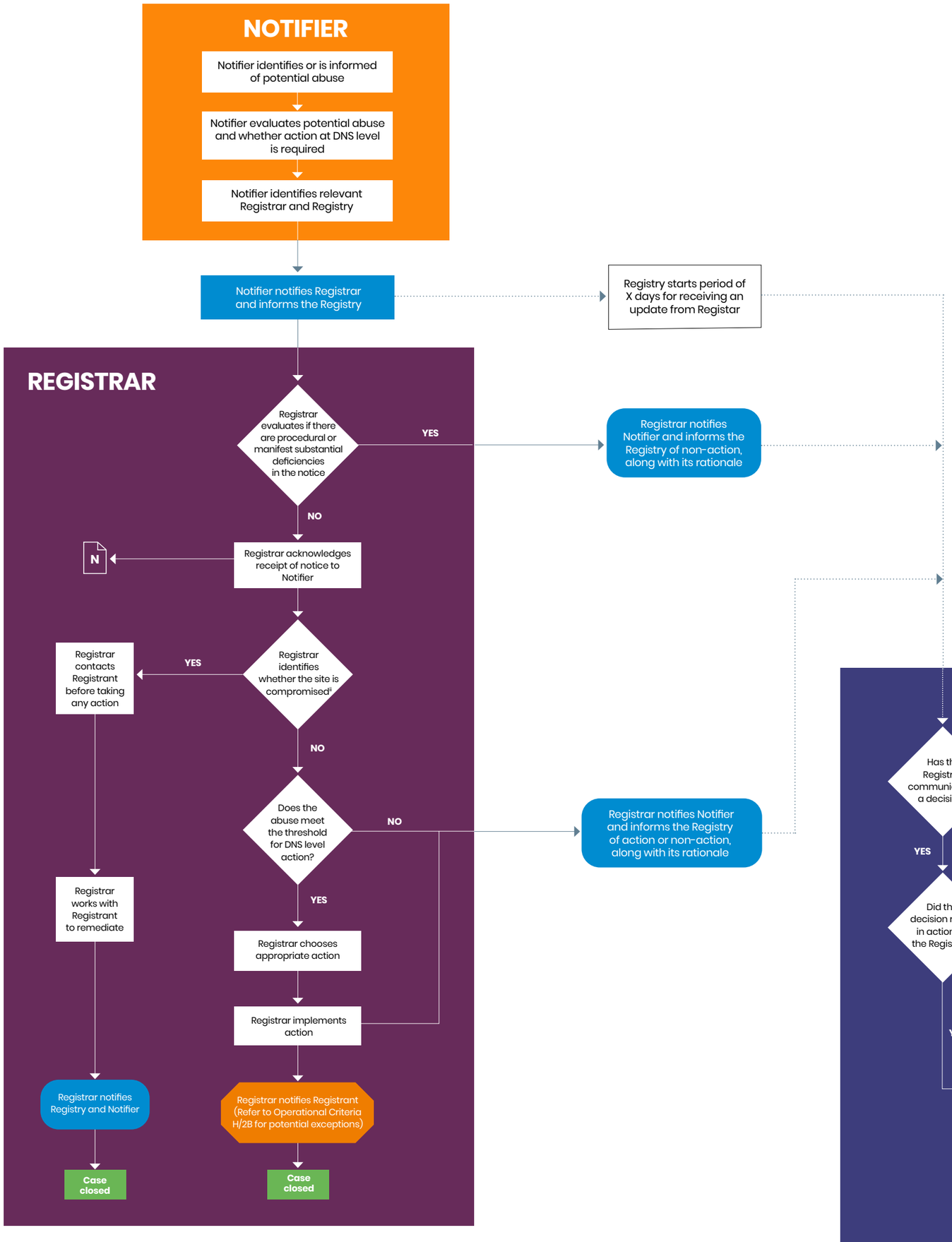
PROCEDURAL WORKFLOW

This section of the Toolkit provides a graphical representation of the procedural workflow for addressing phishing and malware distribution. It visualizes the steps mentioned in the previous stages of this section and provides all actors with a framework to manage their expectations regarding the distribution of responsibilities between actors and the sequence of notifications along the process.

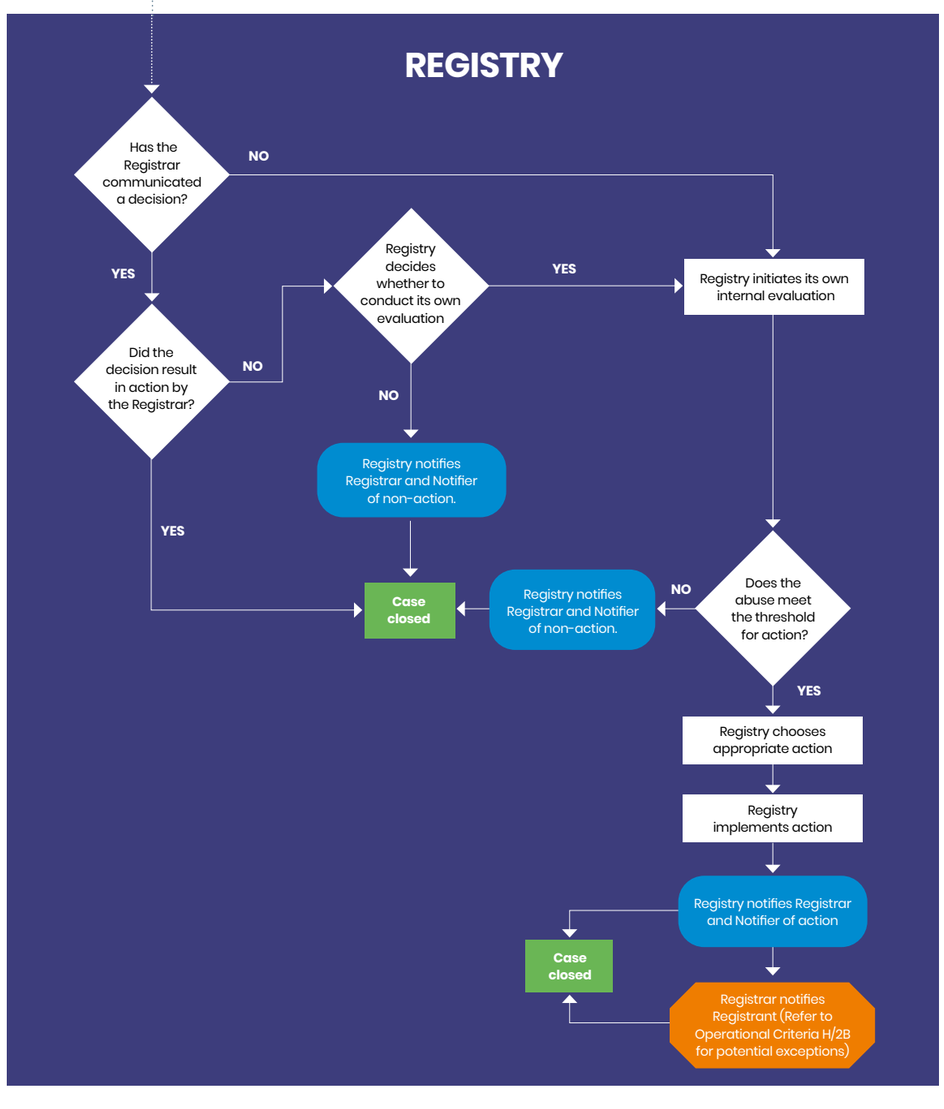
ADDRESSING PHISHING AND MALWARE: A PROCEDURAL WORKFLOW

I&JPN REF: 20-115

This workflow maps the respective roles of Notifiers, Registrars and Registries and the sequence of their interactions.



ii. A domain can be considered compromised not only when the control of the domain is seized by a third party (i.e. someone other than the registrant) and used maliciously to spread malware or conduct phishing, but may also occur in instances where the domain remains under the registrant's control but one or more subpages or URLs are likewise used to propagate phishing or malware without the registrant's knowledge and consent.



1. Abuse report is sent to the Registrar, which has the primary responsibility to investigate and address the abuse report.
2. The Notifier simultaneously informs the Registry (i.e. puts it on copy).
3. The Registrar is expected to decide on action or non-action within a reasonable time frame[i] (e.g. X business days).
4. During this time frame, the Registry is not expected to investigate.
5. The Registrar is expected to inform the Registry and Notifier of its decision to act or not.
6. In case of non communication by Registrar, Registry is expected to initiate its own evaluation.
7. The Registry is expected not to revisit Registrar action but in case of non-action by the Registrar, may conduct its own investigation. The Notifier should be informed of the result of this investigation.
8. The Registrar is expected to notify the Registrant in case of action being taken by either the Registrar or the Registry.
9. Automated ticketing systems can enhance communications and case management.

i. Bilateral arrangements between Registry and Registrar may set specific time lines.

4. INTERNET & JURISDICTION POLICY NETWORK

> **Managing the way that a large number of separate legal frameworks apply to the internet is one of the biggest policy challenges of our time – more complex than building the internet itself.**
>
> **Vint Cerf Co-inventor of the internet, writing in the Financial Times ahead of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in 2018**

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

The regular Global Conferences of the Internet & Jurisdiction Policy Network are institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO. Host partner countries include France (2016), Canada (2018) and Germany (2019).

The Community

6
STAKEHOLDER GROUPS

70+
COUNTRIES

400+
ENTITIES

STATES

INTERNET COMPANIES

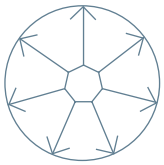
TECHNICAL OPERATORS

CIVIL SOCIETY

INTERNATIONAL ORGANIZATIONS

ACADEMIA

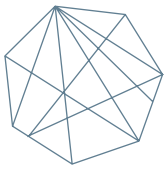
Mission



INFORM

The debates to enable evidence-based policy innovation

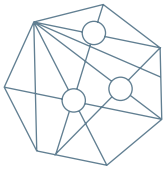
Informational asymmetry and mistrust between actors often result in uncoordinated policy action.
The I&JPN facilitates **pragmatic** and well-informed policy-making by framing issues and taking into account the **diversity of perspectives** while documenting tensions and efforts to address problems.



CONNECT

Stakeholders to build trust and coordination

Cooperation is important in a digital environment that is increasingly polarized, and where actors function in policy silos, with insufficient factual information.
The I&JPN serves as the **connective tissue** between stakeholder groups, regions, and policy sectors, as well as by **bridging gaps** within governments or organizations.



ADVANCE

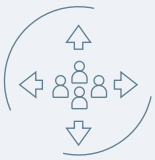
Solutions to move towards legal interoperability

The Policy Network strives to develop shared **cooperation frameworks** and **policy standards** that are as transnational as the internet itself.
The Network promotes a **balanced and scalable approach** to policymaking, aiming for legal interoperability, taking inspiration from the fundamental principle that enabled the success of the internet and the World Wide Web.

Core activities

POLICY PROGRAMS

EVENTS



KNOWLEDGE MUTUALIZATION

5. ACKNOWLEDGEMENTS

This Toolkit is based on the work of the Members of the Domains & Jurisdiction Program Contact Group of the Internet & Jurisdiction Policy Network 2017-2020, and its Outcome Documents, as well as the Roadmaps that resulted from the Global Conferences of the Internet & Jurisdiction Policy Network in 2016 (France), 2018 (Canada) and 2019 (Germany).

The Secretariat is grateful for the hundreds of hours of intense work of the Members of the Domains & Jurisdiction Contact Groups, and their alternates, composed of senior-level representatives from governments, internet companies, technical operators, civil society, leading universities, and international organizations from around the world since 2017.[1] The Secretariat also expresses thanks to the two Contact Group Coordinators between 2017-2020: Maarten Botterman, Director, GNKS Consult and Board Director, ICANN (2017-2019) and Brian Cimbolic, Vice President and General Counsel of Public Interest Registry (2019 - Present).

The following list of Members and their appointed alternates indicates the affiliation of stakeholders at the time they served in the Contact Group. Members served in their personal capacity.

Benedict Addis, Chair, Registrar of Last Resort (RoLR) • **Fiona Alexander**, Distinguished Policy Strategist in Residence, American University • **Gabriel Andrews**, Supervisory Special Agent, Cyber Division - Cyber Initiative & Resource Fusion Unit, Federal Bureau of Investigation • **Mohit Batra**, Technology Analyst, National Internet Exchange of India (NIXI) • **Tijani Ben Jemaa**, Executive Director, Mediterranean Federation of Internet Associations (MFIA) • **James Bladel**, Vice President of Policy, GoDaddy • **Pierre Bonis**, CEO, AFNIC • **Graeme Bunton**, Manager, Analytics and Insights Manager, Public Policy, Tucows • **Brent Carey**, Domain Name Commissioner, .NZ Domain Name Commission • **Jordan Carter**, Chief Executive, InternetNZ • **Mark Carvell**, Head of International Online Policy, United Kingdom - Department for Culture Media and Sport • **Lucien Castex**, Representative for Public Affairs and Partnership Development, AFNIC • **Susan Chalmers**, Internet Policy Specialist, United States - Department of Commerce • **Mishi Choudhary**, Legal Director, Software Freedom Law Centre • **Edmon Chung**, CEO, DotAsia Organisation • **Mason Cole**, Vice President, Communications and Industry Relations, Donuts • **Rocio De La Fuente**, Policy Officer, LACTLD • **Heath Dixon**, Senior Corporate Counsel - Registry, Registrar, and Domains Legal, Amazon Web Services • **Kristine Dorrain**, Senior Corporate Counsel, Amazon Web Services • **Keith Drazek**, Vice President, Public Policy and Government Relations, VeriSign • **Heather Dryden**, Senior Advisor, Canada - Department of Innovation, Science and Economic Development • **Stephanie Duchesneau**, Program Manager, Google • **Miguel Ignacio Estrada**, General Manager, LACTLD • **Rita Forsi**, Director General, Superior Institute for Communications and Information Technology, Italy - Ministry of Economic Development • **Jothan Frakes**, Executive Director, Domain Name Association (DNA) • **Grace Githaiga**, Associate, Kenya ICT Action Network (KICTANet) • **Hartmut Glaser**, Executive Secretary, Brazilian Internet Steering Committee (CGI.br) • **Rahul Gosain**, Director, IRSME, India - Ministry of Electronics and Information Technology • **Rudolf Gridl**, Head of Division, Internet Governance, Germany - Federal Ministry for Economic Affairs and Energy • **Rob Hall**, CEO, Momentous • **Statton Hammock**, Vice President of Global Policy and Industry Development, MarkMonitor • **Jamie Hedlund**, Vice President, Contractual Compliance and Consumer Safeguards, ICANN • **Ashley Heineman**, Director Global Policy, GoDaddy • **Byron Holland**, President and CEO, Canadian Internet Registry Authority (CIRA) • **Will Hudson**, Senior Advisor for International Policy, Google • **Manal Ismail**, Executive Director, International Technical Coordination, Egypt - National Telecommunications Regulatory Authority • **Peter Koch**, Senior Policy Advisor, DENIC • **Konstantinos Komaitis**, Director, Policy Development, Internet Society (ISOC) • **Allan MacGillivray**, Senior Policy Advisor to the President, Canadian Internet Registration Authority (CIRA) • **Marilia Maciel**, Digital Policy Senior Researcher, Diplo Foundation • **Polina Malaja**, Policy Advisor, Council of European National Top-Level Domain Registries (CENTR) • **Fulvia Menin**, Policy

20. An overview of the Members of the Domains & Jurisdiction Program Group by year can be found here.

Officer, European Commission, DG CONNECT • **Julie Michel**, Legal Counsel, EURid • **Desiree Miloshevic**, Senior Advisor of International Affairs and Public Policy, Afilias • **Paul Mitchell**, Senior Director, Technology Policy, Microsoft • **Cristina Monti**, Head of Sector, Internet Governance and Stakeholders' Engagement, European Commission, DG CONNECT • **Alice Munyua**, Founder, Kenya ICT Action Network (KICTANet) • **Michele Neylon**, CEO, Blacknight Internet Solutions • **Seun Ojedeji**, Chief Network Engineer, Federal University of Oye-Ekiti • Crystal Ondo, Policy & Compliance Manager, Google • **David Payne**, Vice President and Deputy General Counsel, Afilias • **Richard Plater**, Policy Executive, Nominet • **Mathieu Potter**, Policy Analyst, Canada - Department of Innovation, Science and Economic Development • **Suzanne Radell**, Senior Policy Advisor, National Telecommunications and Information Administration (NTIA) • **Rod Rasmussen**, Principal, R2 Cyber • **Vinicius Santos**, Expert Advisor, Brazilian Network Information Center (NIC.br) • **Bryan Schilling**, Consumer Safeguards Director, ICANN • **Thomas Schneider**, Head of International Affairs, Switzerland - Federal Office of Communications • **Rowena Schoo**, Policy and Government Relations Manager, Nominet • **Jorg Schweiger**, CEO, DENIC • **Tim Smith**, Executive Director/General Manager, Canadian International Pharmacy Association • **Melina Stroungi**, Policy Officer, European Commission, DG CONNECT • **Hilde Thunem**, CEO, Norid • **Geo Van Langenhove**, Legal Manager & Data Protection Officer, European Registry of Internet Domain Names (EURid) • **Peter Van Roste**, General Manager, Council of European National Top-Level Domain Registries (CENTR) • **Chris Wilson**, Senior Manager, Public Policy, Amazon Web Services • **Alan Woods**, Senior Compliance and Policy Manager, Donuts

I&JPN SECRETARIAT

LEAD DOMAINS & JURISDICTION PROGRAM:

Bertrand de la Chapelle, Executive Director
Elizabeth Behsudi, Director, Domains & Jurisdiction Program
Ajith Francis, Policy Programs Manager
Sophie Tomlinson, Communications and Outreach Manager
Juri Wiedemann, Young Professional

Paul Fehlinger, Deputy Executive Director
Martin Hullin, Director of Operations and Knowledge Partnerships
Hedvig Nahon, Events and Office Manager

FINANCIAL AND INSTITUTIONAL SUPPORTERS

This Toolkit would not exist without the support of the unique coalition of leading states, international organizations, businesses, technical operators and foundations, which enable the work of the Internet & Jurisdiction Policy Network.

Please consult the overview of these key actors and their logos at
https://www.internetjurisdiction.net/about/funding

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

www.internetjurisdiction.net

APPENDIX C

Letter from Michael Binder, Industry Canada, to Robert Hall, CIRA

(11 March 1999)

MAR 11 1999

Mr. Robert Hall
Chair, Canadian Internet Registration Authority
c/o Echelon Internet Corp.
68 Robertson Road
Nepean, Ontario
K2H 8P5

Dear Mr. Hall:

I extend my congratulations to the members of the Board of the Canadian Internet Registration Authority (CIRA) on the recent incorporation of this new not-for-profit organization to administer the .CA domain space on behalf of Canadian users. Industry Canada has attentively followed the continuing efforts to reform the .CA domain name system. Considerable progress has been made to liberalise current registration policies and establish a self-sustaining and viable registry for the .CA Top Level Domain.

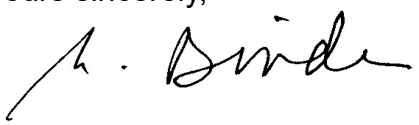
At this important juncture, I would be remiss if I did not offer sincere appreciation to John Demco and the network of dedicated volunteers under whose stewardship the .CA name space has operated for the past decade. The .CA committee's hard work has made a significant contribution towards Canada becoming one of the most "connected" countries in the world. I am now pleased to recognize CIRA as the administrator of the .ca domain space.

The .CA domain space is a key public resource, helping to promote the development of electronic commerce in Canada and important to our country's future social and economic development. As a major user of the .CA domain, as a promoter of the Internet and in its overall policy responsibility for the Information Highway, the Government stated several basic principles for the management of the Internet domain name system in a paper issued in September 1998, entitled "Reform of the Domain Name System - Current Developments & Statement of Principles". We continue to encourage reliance on market forces and private sector leadership in the management of the .CA domain space. Industry Canada expects that the policies CIRA adopts and its operations will be consistent with the principles established by the Canadian government. To this end, we are confident that the CIRA Board will quickly put in place an effective structure predicated upon:

- conducting CIRA's activities in an open and transparent manner that ensures wide public access to all relevant information;
- following fair and sound business practices;
- ensuring an appropriate balance of representation, accountability and diversity on the Board of Directors for all categories of stakeholders;
- applying for domain names being as quick and easy as applying for domain names in other top level domains, and priced competitively;
- reducing conflicts between persons granted domain names and other Fights holders, including trade-marks or business names; and
- a system that facilitates and encourages entry for new players including registrars.

We have a continuing interest in the progress of CIRA. Industry Canada will provide advice and assistance to ensure that the goals pertaining to the administration of the .CA domain name registry are met.

Yours sincerely,



Michael Binder
Assistant Deputy Minister
Spectrum, Information Technologies
and Telecommunications

cc: Members of the CIRA Board of Directors
Esther Dyson, Chair, ICANN
Michael Roberts, President, ICANN
Paul Twomey, Chairman, Government
Advisory Committee, ICANN
Michelle D'Auray, Executive Director,
Electronic Commerce
Task Force, Industry Canada

APPENDIX D

Court File No. A-440-19

FEDERAL COURT OF APPEAL

B E T W E E N:

TEKSAVVY SOLUTIONS INC

APPELLANT

- and -

BELL MEDIA INC, GROUPE TVA INC, ROGERS MEDIA INC, JOHN DOE 1 dba GOLDTV.BIZ, JOHN DOE 2 dba GOLDTV.CA, BELL CANADA BRAGG COMMUNICATIONS INC dba EASTLINK, COGECO CONNEXION INC, DISTRIBUTEL COMMUNICATIONS LIMITED, FIDO SOLUTIONS INC, ROGERS COMMUNICATIONS CANADA INC, SASKATCHEWAN TELECOMMUNICATIONS HOLDING CORPORATION, SHAW COMMUNICATIONS INC, TELUS COMMUNICATIONS INC and VIDEOTRON LTD

RESPONDENTS

CANADIAN INTERNET REGISTRATION AUTHORITY, THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC, FÉDÉRATION INTERNATIONALE DES ASSOCIATIONS DE PRODUCTEURS DE FILMS-FIAPPF, CANADIAN MUSIC PUBLISHERS ASSOCIATION, INTERNATIONAL CONFEDERATION OF MUSIC PUBLISHERS, MUSIC CANADA, INTERNATIONAL FEDERATION OF THE PHONOGRAPHIC INDUSTRY, INTERNATIONAL PUBLISHERS ASSOCIATION, INTERNATIONAL ASSOCIATION OF SCIENTIFIC, TECHNICAL AND MEDICAL PUBLISHERS, AMERICAN ASSOCIATION OF PUBLISHERS, THE PUBLISHERS ASSOCIATION LIMITED, CANADIAN PUBLISHERS' COUNCIL, ASSOCIATION OF CANADIAN PUBLISHERS, THE FOOTBALL ASSOCIATION PREIMER LEAGUE LIMITED, DAZN LIMITED and THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

INTERVENERS

MEMORANDUM OF FACT AND LAW OF THE INTERVENER, CANADIAN INTERNET REGISTRATION AUTHORITY AND OF THE INTERVENER, THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC

Jeremy de Beer Professional Corporation
470 Brierwood Avenue
Ottawa, ON K2A 2H3

Jeremy de Beer

Tel: +1 613-263-9081
Email: jeremy@JeremyDeBeer.ca

Counsel for the Intervener, Canadian Internet Registration Authority (CIRA)

32M Law Professional Corporation
395 Montrose Ave.
Toronto, ON M6G 3H2

Bram Abramson

Tel: +1 647-680-8354
Email: bram@32M.io

Counsel for the Intervener, Canadian Internet Registration Authority (CIRA)

Caza Saikaley SRL/LLP
#250-220 Laurier Avenue West
Ottawa, ON K1P 5Z9

Alyssa Tomkins (atomkins@plaideurs.ca)
James Plotkin (jplotkin@plaideurs.ca)

Tel: +1 613-565-2292
Fax: +1 613-565-2087

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tamir Israel

Tel: +1 613-562-5800 ext 2914
Fax: +1 613-562-5417
Email: tisrael@cippic.ca

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

TO:	**OFFICE OF THE REGISTRY** **FEDERAL COURT OF APPEAL**
AND TO:	**CONWAY BAXTER WILSON LLP/SRL** #400-411 Roosevelt Avenue Ottawa, ON K2A 3X9 Colin Baxter (cbaxter@conway.pro) Marion Sandilands (msandilands@conway.pro) Julie Mouris (jmouris@conway.pro) Tel: +1 613-288-0149 Fax: +1613-688-0271 **Counsel for the Appellant, Teksavvy Solutions Inc**
AND TO:	**SMART & BIGGAR LLP** #3300-1000 de la Gauchetière Street West Montréal, QC H3B 4W5 François Guay (fguay@smartbiggar.ca) Ryan T Evans (REvans@smartbiggar.ca) Guillaume Lavoie Ste-Marie (GLavoieSteMarie@smartbiggar.ca) Olivier Jean-Lévesque (OJean-Levesque@smartbiggar.ca) Tel: +1 514-954-1500 Fax: +1 514-954-1396 **Counsel for the Respondents, Bell Media Inc, Groupe TVA Inc, Rogers Media Inc, Bell Canada, Fido Solutions Inc, Rogers Communications Canada Inc and Videotron Ltd**
AND TO:	**GIB VAN ERT LAW** 148 Third Avenue Ottawa, ON K1S 2K1 Gib van Ert Tel: +1 613-408-4297 Fax: +1 613-651-0304 Email: gib@gibvanertlaw.com **Counsel for the Intervener, British Columbia Civil Liberties Association (BCCLA)**
AND TO:	**MACKENZIE BARRISTERS PC** Richmond Adelaide Centre 120 Adelaide Street West, Suite 2100 Toronto, ON M5H 1T1

	Gavin MacKenzie (gavin@mackenziebarristers.com) Brooke MacKenzie (brooke@mackenziebarristers.com) Tel: +1 416-304-9293 Fax +1 416-304-9296 **Counsel for the Intervener, Fédération Internationale de Producteurs de Films—FIAPF**
AND TO:	**CASSELS BROCK & BLACKWELL LLP** 2100 Scotia Plaza 40 King Street West Toronto, ON M5H 3C2 Casey Chisick (cchisick@cassels.com) Eric Mayzel (emayzel@cassels.com) Tel: +1 416-869-5403 Fax: +1 416-644-9326 **Counsel for the Intervener, Canadian Music Publishers Association, International Confederation of Music Publishers, Music Canada, and International Federation of the Phonographic Industry**
AND TO:	**MCCARTHY TÉTRAULT LLP** TD Bank Tower 66 Wellington Street West, Suite 5300 Toronto ON, M5K 1E6 Barry Sookman (bsookman@mccarthy.ca) Steven Mason (smason@mccarthy.ca) Dan Glover (dglover@mccarthy.ca) Bruna Kalinoski (bkalinoski@mccarthy.ca) Tel: +1 416-362-1812 Fax: +1 416-868-0673 **Counsel for the Interveners, International Publishers Association, International Association of Scientific, Technical and Medical Publishers, American Association of Publishers, the Publishers Association Limited, Canadian Publishers' Council, Association of Canadian Publishers, the Football Association Premier League Limited and Dazn Limited**

TABLE OF CONTENTS

PART I - STATEMENT OF FACT

1. The interveners submit three reasons for restraint when courts are asked to order common carriers to block Internet communications. CIPPIC submits (A) ISP-based blocking remedies disrupt the *Copyright Act*'s balanced intermediary enforcement regime. CIRA submits (B) telecommunications law constrains the power to order blocking; and (C) detailed statutory schemes limit blocking norms and practices abroad.

PART II - ISSUES

2. The issues are as framed in the Appellant's memorandum of fact and law.

PART III - SUBMISSIONS

A. The *Copyright Act*'s intermediary enforcement regime excludes ISP blocking.

A.1 Equitable discretion must be informed by implicated legal regimes.

3. When exercising discretion to issue injunctive relief, courts must consider relevant statutory and common law. *RJR–Macdonald* provides only a "general framework"[1] that, to borrow a phrase from administrative law, takes its "colour from the context".[2]

4. That courts must tailor their equitable authority to the specific legal circumstances is uncontroversial. Sometimes the contextual criteria are express, as with labour injunctions where the applicant must demonstrate reasonable efforts to obtain police assistance before seeking an injunction.[3] Other times the criteria are jurisprudential. This Court will deny an interlocutory injunction in a patent or industrial design case where infringement and validity are in issue and the defendant undertakes to account.[4] Implicated statutory schemes such as the *Copyright Act* and the *Telecommunications Act* likewise provide guidance through their respective text, context and purpose, as canvassed below.[5]

5. Before addressing the copyright context, it is important to note that the court cannot merely state it concludes the plaintiff has a strong *prima facie* case. Reasons are the primary mechanism by which judges account to parties, the public and appellate courts for their decisions.[6] As observed in the administrative law context—where procedural

---

1 *R v Canadian Broadcasting Corp*, [2018] 1 SCR 196, 2018 SCC 5, ¶13 (*CBC*).
2 *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, ¶89 [*Vavilov*]; *Warman v Fournier*, 2012 FC 803, ¶¶18-21 [*Fournier*].
3 See for example: *Courts of Justice Act*, RSO 1990, c C.43, s 102(3).
4 *Apotex Inc v Bayer Inc*, 2018 FCA 32, ¶51, [2018] 4 FCR 58.
5 See for example: *Théberge v Galerie d'Art du Petit Champlain Inc*, [2002] 2 SCR 336, 2002 SCC 34, [*Théberge*] per Gonthier, J, dissenting, but not on this point, ¶¶101-102; *Fournier*, ¶¶18-21.
6 *R v Sheppard*, [2002] 1 SCR 869, 2002 SCC 26, ¶15.

fairness requirements are "eminently variable" and generally, if not always, lower than the judicial standard—the reasons must provide "[e]*nough information…so parties can assess whether or not to exercise their rights of review, the supervising court can review what has been done, and the public can scrutinize what has happened*."[7] This requirement is arguably heightened in a judicial setting involving an exceptional remedy.

A.2 General remedial powers cannot undermine limits on copyright remedies.

6. The 'colour' that *Copyright Act* provisions bring to the court's general remedial powers emerges from the *Act*'s purpose: to provide a "*balance between promoting the public interest in…dissemination of works…and obtaining a just reward for the creator*" or, specifically, a balance between the rights of users and copyright holders.[8] Provisions within the *Act* must therefore be read not only in terms of what is expressly granted to copyright holders, but also what is withheld.[9] This context bears on whether and how general statutory[10] and common law[11] powers interface with the *Act*.

7. The balance principle must inform the common law's application to copyright matters, regardless of whether that common law is expressly referenced in the Act or another statute.[12] For example, the Supreme Court has held that section 12 of the *Act*, which generally preserves common law Crown prerogative, must accord with the balance at the heart of the *Act*.[13] Similarly, this Court held that provisions in the *Interpretation Act* recognizing a common law presumption of Crown immunity cannot interfere with one of the *Copyright Act*'s detailed and balanced statutory schemes.[14]

---

7 *Vavilov*, ¶76-81; *Vancouver International Airport Authority v Public Service Alliance of Canada*, 2010 FCA 158, ¶15.

8 *Théberge*, ¶30; *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers*, [2004] 2 SCR 427, 2004 SCC 45, [*SOCAN*] ¶¶88-89; *CCH Canadian Ltd v Law Society of Upper Canada*, [2004] 1 SCR 339, 2004 SCC 13 [*CCH*]; *Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2020-168*, [2012] 3 SCR 489, 2012 SCC 68, [*Reference re Broadcasting*] ¶¶64-66; *Entertainment Software Assoc v Society Composers*, 2020 FCA 100, ¶67.

9 *Théberge*, ¶31; *Reference re Broadcasting*, ¶66. *Charter*, section 2(b) also protects listeners as well as speakers: Intervener, British Columbia Civil Liberties Association, Memorandum of Fact and Law.

10 For example, open-ended powers of a subordinate regulator: *Reference re Broadcasting*, ¶¶64-66.

11 *Reference re Broadcasting*, ¶¶59, 67 and 78; *Fournier*, ¶18-21.

12 E.g. compare s 34.1 (general discretionary injunctive relief) and ss 41.27 (3) and (4.1)(specific regime for injunctions against information location tools).

13 *Keatley Surveying Ltd v Teranet Inc*, 2019 SCC 43, ¶¶42, 47 and 48.

14 *Manitoba v Canadian Copyright Licensing Agency (Access Copyright)*, 2013 FCA 91 [*Access Copyright*].

8. Even absent conflict with an express provision general powers, such as the open-ended equitable relief under appeal, cannot disturb the balance struck in the *Act*.[15] Courts respect this balance by examining specific provisions with careful attention to their context and underlying purpose. In *Reference re Broadcasting*, the Supreme Court struck down use of a general regulatory power to grant copyright holders control over distribution undertaking signals retransmission.[16] Failing to include these undertakings in a detailed *Copyright Act* scheme governing control over broadcaster retransmission was sufficient to create an implicit user right—one that could not be dislodged by a general power.[17]

9. Courts are especially hesitant to rely on general powers if doing so would interfere with how the *Act* allocates control over communication of subject matter. Encouraging the dissemination of works is one of the *Act*'s core concerns, and one of its two driving purposes.[18] This core concern encompasses not only control granted to copyright holders over communication of subject matter, but also any limits on that control. Such limits constitute users' rights to receive subject matter over particular communication networks.[19]

10. This framework applies to remedial powers of general application, including the equitable injunctive power at issue here. For example, the *Act* expressly recognized courts' inherent interlocutory powers to seize copyright-infringing works before judgment. The *Act* does not specify, however, whether this general remedy extends to moral rights infringements.[20] In *Théberge*, the Supreme Court interpreted the *Act*'s silence to preclude seizure as a moral rights remedy, in part due to the remedy's highly intrusive nature.[21] Courts likewise cannot order the remedy at issue here without considering its intrusive impact on the balance struck in the intermediary-based enforcement regime outlined below.

---

15 *Reference re Broadcasting*, ¶¶63-64 and 67, 70, 78; *Access Copyright*, ¶48; *Fournier*, ¶¶18-21: ("It would be contrary to Parliament's intent to find that an injunction is presumptively available for an infringement if the application is brought outside the limitation period.").

16 *Reference re Broadcasting*, ¶¶29-32, and 78.

17 *Reference re Broadcasting*, ¶¶59, 63-64, 67, 70 and 78.

18 *Bell Canada v Canada (AG)*, 2017 FCA 249, ¶¶45-46, rev'd on other grounds, 2019 SCC 66.

19 *Reference re Broadcasting*, ¶¶63-64, 67, 70, 75 and 78: "copyright owners 'should not be permitted to stop retransmission because this activity is too important to Canada's communications system.'"

20 *Théberge*, per Binnie, J, ¶¶76-79 and per Gonthier, J, dissenting, ¶¶129-134.

21 *Théberge*, ¶78.

A.3 ISP-based blocking unbalances the copyright intermediary enforcement regime.

11. The *Copyright Act* encodes balance in a detailed regime that articulates specific roles for different intermediaries.[22] Parliament recognised the need to restrict copyright holders' control over the distribution of infringing subject matter, and the corresponding users' right to receive works through a particular sort of intermediary. The balance struck in these provisions reflects Parliament's awareness of the different and intrusive impact that results when Internet Service Providers ("ISP") are used to remove infringing content. These remedies therefore should only issue as a last resort or, better still, be left to Parliament.

12. An intermediary is defined as an entity providing the "means" of communicating works in a 'neutral' manner.[23] The intermediary regime adopted in the *Copyright Modernization Act* addresses three categories of intermediaries: search engines (Information Location Tools), content hosts (digital memory providers) and ISPs (Network Service Providers).[24] Of these, only ISPs are common carriers, subject to common law and *Telecommunications Act* requirements and liability immunities designed to limit interference with content.[25]

13. This intermediary regime contains several detailed components. Responding to the Supreme Court's invitation, Parliament clarified the liability and remedy exposure of ISPs and encoded the common law concept of 'authorization' as applicable to different intermediaries.[26] The *Act* similarly establishes specific contexts in which rights holders can enlist intermediaries to assist in rights enforcement tasks.

14. This regime demonstrates that the balance Parliament struck between competing rights strongly disfavours the use of intermediaries as removal tools for infringing content[27]—particularly so if the intermediary is an ISP. The injunctive relief expressly provided against search engines further implies that the remedy under appeal is unavailable.

---

22 *Rogers Communications Inc v Voltage Pictures LLC*, [2018] 2 SCR 643, 2018 SCC 38, [*Voltage*] ¶¶22-25.

23 *SOCAN*, ¶92; *Bell Canada v Lackman*, 2018 FCA 42 [*Lackman*], ¶¶23-27.

24 *Copyright Act*, RSC 1985, c C-42, ss 41.25(1)(a)-(c).

25 See discussion in Section B, below; *Electric Despatch co of Toronto v Bell Telephone Co of Canada*, (1891) 20 SCR 83; *Dominion Telegraph Company v Silver*, (1882) 10 SCR 238, and Law Commission of Ontario, "Defamation Law in the Internet Age", March 2020 [LCO], p 74.

26 *SOCAN*, ¶127; *Voltage*, ¶27; *Copyright Modernization Act*, SC 2010, c 20, "This enactment amends the *Copyright Act* to…clarify Internet service providers' liability"; Testimony of Craig McTaggart, Director, Broadband Policy, TELUS, House of Commons Legislative Committee on Bill C-32, 40(3), March 22, 2011, 1100; *Copyright Act*, s 27(2.3).

27 *Théberge*, ¶78; *SOCAN*, ¶101; *Reference re Broadcasting*, ¶¶66-67 & 70; *Fournier*, ¶¶18-21.

15. **Liability & Remedy Limitations.** The *Act* removes liability where ISPs, in operating digital network access services, provide the means for individuals to reproduce or telecommunicate protected subject matter.[28] It similarly removes liability for content hosts who provide digital memory where individuals store protected subject matter for the purpose of communicating it over digital networks.[29] The liability of search engines is not so limited. Instead, the *Act* restricts remedies available against search engines found liable for copyright infringement.[30] Authorization is also codified by the *Act*, which limits the liability and remedy in instances where the intermediary is found to be an 'enabler' of copyright infringement.[31] These liability and remedial limitations voice Parliament's indication that intermediary liability would lead to disproportionate content removal.[32]

16. **Codified Intermediary Enforcement Actions.** The *Act* explicitly encodes a robust set of intermediary actions that copyright holders can engage to enforce their rights.[33] Content hosts and ISPs must forward notices of alleged infringement to customers, and preserve customer information within their control so copyright holders can pursue the primary infringer if they wish.[34] Remedies against intermediaries who fail to meet their notice-forwarding or data preservation obligations are limited to statutory damages.[35]

17. **Removal Obligations.** The *Act* explicitly recognizes specific intermediary enforcement actions that lead to removal of infringing content. These include:

    - **Search Engines**: Where a search engine hosts a copy of content originally hosted elsewhere, it must remove that copy within 30 days of receiving a notice of claimed infringement if the work has already been removed from its original location.[36] If it fails to comply, it loses the remedy limitation granted by the *Act*.
    - **Search Engines**: Search engines found liable for copyright infringement are subject to first party injunctions, but remain immunized from other remedies.[37] A first party injunction against an infringing search engine can only issue if the

---

28 *Copyright Act*, ss 31.1(1)-(3).
29 *Copyright Act*, s 31.1(4).
30 *Copyright Act*, ss 41.27(1)-(2) and (5).
31 *Copyright Act*, ss 27(2.3)-(2.4), 31.1(6) & 41.27(4); *SOCAN*, ¶127; *Lackman*, ¶¶28-36; *Voltage*, ¶27.
32 *SOCAN*, ¶127. See footnote 26, above and LCO, p 74.
33 *Voltage*, ¶¶22-25.
34 *Copyright Act*, ss 41.25(1)(a)-(b) and 41.26(1)(a) & (b), respectively. *Voltage*, ¶6.
35 *Copyright Act*, s 41.26(3); *Voltage*, ¶27.
36 *Copyright Act*, s 41.27(3).
37 *Copyright Act*, s 41.27(1).

copyright holder can establish a list of prescribed factors including that no less burdensome and comparably effective means are available.[38] Wide injunctions are never available as a remedy against search engines.[39]

- **Content Hosts:** A content host must remove copyrighted material if it is aware (or made aware) of a court decision holding that the individual storing the content in its digital memory has done so by infringing copyright.[40] If it fails to comply, it loses the liability limitation granted to it by the *Act*.

Within this scheme, the *Act* recognizes limited content removal obligations against search engines and content hosts, but none against ISPs. Parliament was urged to encode third-party injunctive relief against all intermediaries based on international examples.[41] Instead it opted for first-party injunctive relief against search engines only, while clarifying that ISPs have no liability whatsoever.[42] While not explicitly foreclosing ISP injunctions, this scheme recognizes the more intrusive nature of content removal remedies issued against ISPs as opposed to other types of intermediaries in other legislative contexts, distinguishing it from the remedy issued in decisions such as *Equustek*.[43]

18. The injunction issued below is not consonant with the balance struck in this legislative scheme. The *Act* articulated specific contexts providing for intermediary assistance in enforcement, representing a balance between the interests of copyright holders and the rights of users.[44] The *Act* specifically outlines conditions in which copyright holders can prevent intermediaries from facilitating the dissemination of infringing subject matter.[45] The absence of any power to control ISP-based dissemination of infringing subject matter at all is, within the scheme of the *Act*, a users' right to ISP-based dissemination.[46]

---

38 *Copyright Act*, s 41.27(4.1).
39 *Copyright Act*, ss 39.1 and 41.27(4.2).
40 *Copyright Act*, s 31.1(5).
41 Canadian Music Publishers Association, C-11 Submission, November 29, 2011, pp 9-12; Testimony of Catharine Saxberg, Executive Director, Canadian Music Publishers Association, C-11 Committee, House of Commons Legislative Committee on Bill C-11, 41(1), March 6, 2012, 0905.
42 *CCH*, ¶¶5 & 85-86 (no s 34(1) injunctive relief available in absence of liability); House of Commons, Legislative Committee on Bill C-11, CC11 Committee Report, 41(1). March 15, 2012, Cl 47(f).
43 *Google Inc v Equustek Solutions Inc*, [2017] 1 SCR 824, 2017 SCC 34 [*Equustek*]; *Crookes v Newton*, [2011] 3 SCR 269, 2011 SCC 47, ¶21; LCO, pp 72-75.
44 *Copyright Act*, ss 31.1 & 41.25-41.27. *Reference re Broadcasting*, ¶¶63-64 and 67, 70, 78; *Access Copyright*, ¶48; *Fournier*, ¶¶18-21; *Théberge*, ¶¶30 and 78.
45 *Copyright Act*, ss 31.1(5), 41.27 (1), (3), (4.1) and (4.2); *Reference re Broadcasting*, ¶75: *SOCAN*, ¶¶88-89; *Bell Canada v Canada (AG)*, 2017 FCA 249, ¶¶45-46, rev'd on other grounds, 2019 SCC 66.
46 *SOCAN*, ¶¶88-89; *Reference re Broadcasting*, ¶¶63-64, 67, 70, 75 and 78.

19. Finally, in contrast to other statutory contexts,[47] the first-party injunctive relief against search engines will only issue where the copyright holder establishes harm of sufficient severity,[48] and only as a last resort.[49] Further, search engines cannot be required by first-party injunction to remove infringing subject matter not explicitly pleaded.[50] The unavailability of wide injunctions effectively limits relief against search engines to the removal of specific online locations associated with specific infringing works explicitly before the court.[51] The order issued against GoldTV is a first-party wide injunction as it enjoins the defendants from communicating any of the plaintiffs' works, not only those explicitly identified in their pleadings.[52] In contrast, the injunction under appeal, itself contingent on that order, is even wider in scope as it prevents the defendants from communicating *any* subject-matter—or anything *at all*—through named ISPs.[53]

20. Relying on a general remedial power to create a new remedy against an ISP substantially disrupts the balance carefully struck by Parliament by ignoring its hesitance to rely on ISPs for content removal and its prohibition of wide injunctions against search engines. The limits placed on the intermediary enforcement regime are "important element[s] of the balance struck by the statutory copyright scheme"—they constitute a user right, "not a loophole".[54] Parliament "had good reason not to authorize"[55] such a remedy. This Court, as a court of law and equity, should therefore decline to exercise its discretion to do so.

21. The critical and intersecting role of the *Telecommunications Act*, which places additional limitations on blocking by common carriers such as ISPs, reinforces this conclusion.

---

47 *Microsoft Corp v 9038-3746 Ontario Inc*, 2006 FC 1509, ¶¶130 & 136-138; *Equustek*, ¶8.

48 *Copyright Act*, s 41.27(4.1)(a). Contrast *Bell Media Inc v GoldTV.Biz*, 2019 FC 1432, [GoldTV] ¶¶66-67.

49 *Copyright Act*, s 41.27(4.1)(b)(iv). Contrast *GoldTV*, ¶¶64-65.

50 *Copyright Act*, ss 41.27(4.2) & 39.1; *Thomson v Afterlife Network Inc*, 2019 FC 545 [*Afterlife*], ¶¶49-54; *Trader v CarGurus*, 2017 ONSC 1841 [*CarGurus*], ¶¶69-71; *Microsoft Corp v 127916 Ontario Ltd*, 2009 FC 849, ¶52; *Microsoft Corporation v 9038-3746 Ontario Inc*, 2006 FC 1509, ¶136.

51 By contrast, see *Equustek Solutions Inc v Jack*, 2014 BCSC 1063, ¶9.

52 Order of Justice LeBlanc, FC File No T-1169-19, July 25, 2019, clauses 1(a)(iv)-(v) and (b)(iv)-(v): "(the "Plaintiffs Programs", examples of which are listed in Appendix 1 hereto)".

53 *Afterlife*, ¶¶49-54; *CarGurus*, ¶¶69-71. By contrast, first party wide injunctions are available if the conditions in s.39.1 are met: *Nintendo of America v King*, 2017 FC 246, ¶¶175-177; contrast: *Bell Canada v 1326030 Ontario Inc (iTVBox.net)*, 2016 FC 612, ¶33, aff'd 2017 FCA 55; and *Wenham v Canada (Attorney General)*, 2018 FCA 199, ¶¶43-44.

54 *SOCAN*, ¶¶89-90, 92, 101 and 127; *Fournier*, ¶¶18-21.

55 *Théberge*, ¶78; *SOCAN*, ¶127: "A more effective remedy to address this potential issue would be the enactment by Parliament of a statutory ... procedure as has been done in the European Community and the United States."

B. Telecommunications law constrains the power to order blocking.

B.1 Copyright and telecommunications law must be interpreted harmoniously.

22. The *Telecommunications Act*[56] and related Cabinet regulations[57] establish a polycentric telecommunications policy and delegate powers to the Canadian Radio-television and Telecommunications Commission (CRTC) to further that policy. To this end, section 36 of the *Telecommunications Act* requires that a common carrier not "control or influence" the telecommunications it carries "[e]xcept where the Commission approves otherwise". Blocking internet traffic controls or influences telecommunications.[58] Yet the decision appealed suggests that telecommunications law does not constrain the courts' jurisdiction or discretion to order blocking without CRTC approval (¶42, ¶¶96-97) nor allow the CRTC to "interfere" with such an order (¶41, citing *Reference re Broadcasting*).

23. *Reference re Broadcasting* did establish that the CRTC cannot create an entirely new regulatory regime that operationally conflicts or is incompatible with the purposes of applicable legislation.[59] Here, however, there need be no such conflict or incompatibility. Rather than relegate either telecommunications or copyright law to secondary status, courts ought to interpret both statutes to stand together harmoniously.

24. The issue in the CRTC's FairPlay decision was also different than here. The CRTC correctly found in FairPlay that it cannot mandate blocking as a copyright remedy under sections 24 and 24.1 of the *Telecommunications Act*.[60] But, as it previously decided, the CRTC can and must review and authorize blocking under section 36.[61]

25. Instead of reasoning that the Court's general ability to grant copyright remedies leaves no

---

56 SC 1993, c 38, s 7.

57 *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, SOR/2006-355 [*Policy Direction (2006)*]; *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives to Promote Competition, Affordability, Consumer Interests and Innovation*, SOR/2019-227 [*Policy Direction (2019)*].

58 *Review of the Internet traffic management practices of Internet service providers*, Telecom Regulatory Policy CRTC 2009-657, 21 October 2009, ¶121-22.

59 *Reference re Broadcasting*, ¶¶39, 45.

60 *Application to disable online access to piracy websites*, Telecom Decision CRTC 2018-384, 2 October 2018, ¶¶60-62, 67.

61 *Application for relief regarding section 12 of the Quebec Budget Act*, Telecom Decision CRTC 2016-479, 9 December 2016, ¶¶7, 18-21 [*Re Quebec Budget Act*]; *Decision re application of Richard Warman*, Telecom Commission Letter 8622-P49-200610510, 24 August 2006.

room for the *Telecommunications Act*, consider how telecommunications law requires policy scrutiny of certain copyright remedies. That is how the relevant statutes can be, as Justice Rothstein emphasized in *Reference re Broadcasting*, "read together so as to *avoid* conflict".[62] A coherent, harmonious statutory interpretation requires review of applications for blocking orders against the telecommunications policy objectives Parliament enacted[63] by the body Parliament tasked[64] or, at least, by the courts.

B.2 The legislative text, context, and purpose require policy scrutiny of blocking.

26. Subordinating or ignoring telecommunications law contravenes the text, context, and purpose of the statute and regulations. The requirement to act "solely as a common carrier" and not "control the contents nor influence the meaning or purpose" of telecommunications, first in the *Bell Canada Special Act*[65] and then in section 36 of the *Telecommunications Act*, exists in the context of the common carrier's obligation to avoid discrimination. Section 36's chapeau captures the concept as: "neutralité quant au contenu". Decisions as to when such discrimination furthers the purposes of the *Act*, clearly stated in sections 7 and 8, are expressly delegated to the CRTC under section 47.

27. The CRTC understood this scheme when it required prior regulatory review of a program for Bell Canada to block "access by minors to programmes that contain descriptions of sexual conduct".[66] The CRTC confirmed this scheme recently, deciding that even if ISPs are compelled by an otherwise-valid legal obligation to block unlicensed gambling sites, "the Act prohibits" such blocking "without prior Commission approval", to be granted "only … where it would further the telecommunications policy objectives".[67]

28. This scheme is not unusual in respect of common carriers.[68] It leaves room for the courts to adjudicate and remedy copyright infringement. But it also leaves room to apply the *Telecommunications Act* in reviewing those rare remedies that require telecommunications common carriers to interfere in the content they carry.

---

62 *Reference re Broadcasting*, ¶38, emphasis by Rothstein J.
63 *Telecommunications Act*, ss 7, 8, 47 and 36.
64 *Telecommunications Act*, s 36 (delegation to "the Commission").
65 SC 1967-68, c 48, s 6, adding s 5(3) to SC 1948, c 81.
66 *Re 976 Services – Billing and Collection*, Telecom Letter Decision CRTC 92-5, 26 June 1992.
67 *Re Quebec Budget Act*, Telecom Decision CRTC 2016-479, 9 December 2016, ¶¶7, 18-21.
68 See, similarly, *Canada Post Corporation Act*, RSC 1985, c C-10, ss 43-47, assigning review of postal delivery-blocking to a Minister-appointed Board of Review.

29. Evidence "to the effect that the cost of implementation and the exclusion of some third party ISPs from the scope of the order will potentially negatively impact the competitive position of smaller ISPs including Teksavvy" (¶98) must be weighed against telecommunications policy objectives. Specifically, would the order: "render reliable and affordable telecommunications services of high quality accessible to Canadians"; "promote the use of Canadian transmission facilities for telecommunications within Canada and between Canada and points outside Canada"; "foster affordability and lower prices, particularly when telecommunications service providers exercise market power"; and "reduce barriers into the market and to competition"?[69]

30. Similarly, "assertions of a negative competitive impact" (¶99) must be assessed not only in this narrow context but also considering telecommunications policy concerns with the vertical integration of common carriers and content providers. As put by a 2019 Parliamentary committee considering blocking orders: "It is not hard to imagine a situation where one vertically integrated ISP-rights-holder seeks an injunction that would apply to another ISP-rights-holder, who would gladly provide it with little contest given that they share similar interests in the outcome of the case."[70] Here, related companies predominated as both the applicants seeking the remedy and the third-party common carriers implementing it. Apprehension of such difficulties, and how to weigh them against polycentric telecommunications objectives, is exactly the role Parliament assigned to the CRTC for review and approval of telecommunications blocking.[71]

C. Detailed statutory schemes limit blocking norms and practices abroad.

C.1 International law leaves room for Parliament's distinct enforcement scheme.

31. Copyright treaties say nothing about blocking orders, injunctions against ISPs, or online intermediaries' role in copyright enforcement. The WIPO Internet Treaties, for example, require parties to ensure that "enforcement procedures … permit effective action against any act of infringement … including expeditious remedies to prevent infringements."[72]

---

69 *Telecommunications Act*, ss 7(b), 7(e), 8, 47(b); *Policy Direction (2019)*, ss 1(a)(ii), (v).

70 *Statutory Review of the Copyright Act*, Report of the Standing Committee on Industry, Science, and Technology, House of Commons, 42nd Parl, 1st S, pp 97-98.

71 See CRTC, Navigating Convergence, February 2010, s 4.2.

72 WIPO Copyright Treaty, 20 December 1996, 2186 UNTS 121 at 156, art 14(2) (entered into force 5 March 2002); WIPO Performances and Phonograms Treaty, 20 December 1996, 2186 UNTS 203 at 253, art 23(2) (entered into force 19 May 2002).

But those general words cannot now be contorted as a "make-weight" for interpreting domestic laws.[73] Moreover, there is no recognized legal norm, customary rule, or state practice constituting public international law on blocking orders. To the contrary, Canada's recent trade deals reinforce Parliament's intent about blocking. For example, the Canada United States Mexico Agreement expressly permits Canada to preserve the distinctive approach to different intermediaries' role in copyright enforcement established by the 2012 statutory reforms, from which blocking is conspicuously absent.[74]

C.2 Other jurisdictions base blocking orders on explicit statutory regimes.

32. Comparative legal analysis can help distinguish foreign blocking schemes from Canadian law. Where legislators prescribed statutory reforms, such as in Australia, the United Kingdom (UK), and elsewhere in the European Union (EU), courts grant blocking orders. Where legislators considered and rejected a statutory scheme for site blocking, such as in the United States (US), courts typically do not.

33. A blocking scheme was proposed in the United States in a pair of 2011 bills detailing how applications would work, including threshold criteria and tailored measures for different classes of intermediaries.[75] The controversial bills did not become law. As such, ISP-based blocking in the US is contemplated only under an explicit, narrow provision with limited scope.[76] Because American courts have not generally endorsed blocking orders, copyright owners in the United States are asking legislators for statutory reform.[77]

34. In contrast to the US and Canada, Australian legislation is "deliberately prescriptive; it is intended as a precise response to a specific concern raised by copyright owners."[78]

---

73 *Entertainment Software Assoc v Society Composers*, 2020 FCA 100, ¶76.

74 Agreement Between the United States of America, the United Mexican States, and Canada, 30 November 2018, Annex 20-B (Annex to Section J), p 62; *Canada-United States-Mexico Agreement Implementation Act*, SC 2020, c 1; *Copyright Modernization Act*, SC 2012, c 20.

75 US, Bill HR 3261, *Stop Online Piracy Act*, 2011, §§102-104; US, Bill S 968, *PROTECT IP Act*, 112th Cong, 2011, §3(d)(2).

76 US, *Digital Millennium Copyright Act*, 17 U.S.C. §512(j)(1)(B)(ii). Some US orders against first-party defendants purport to bind non-parties who are "in active concert or participation" with defendants under *Federal Rules of Civil Procedure* Rule 65(d)(2)(C) or the *All Writs Act*, 28 USC §1651.

77 US, *Hearing on Approaches to Foreign Jurisdictions to Copyright Law and Internet Piracy Before the US Senate Committee on the Judiciary*, 116th Cong, 10 March 2020 (Stanford K. McCoy).

78 Austl, Commonwealth, Senate, *Copyright Amendment (Online Infringement) Bill 2015*, *Revised Explanatory Memorandum*, (2015), ¶1.

Section 115A of Australia's copyright statute—enacted in 2015[79] after human rights and financial assessments, and tweaked in 2018[80] to address unforeseen consequences—sets "an intentionally high threshold test".[81] The remedial powers in the *Federal Court of Australia Act 1976*[82] are as broad as in Canada's *Federal Courts Act*. And like Canada, the principles of equity evolved in Australia from common UK traditions. But Australia's Parliament was nonetheless compelled to legislate a specific regime for blocking orders.

35. Australia's statutory scheme cross-references the definition of "carriage service provider" to the *Telecommunications Act 1997* to promote consistency with telecommunications law.[83] Separately, an "online search engine provider" may be ordered to take reasonable steps to not refer users to an online location. In comparison, the courts in Canada would need to reconcile (or ignore) the *Telecommunications Act*'s and *Copyright Act*'s rules differentiating "information location tools", for which blocking injunctions are explicitly contemplated, from "providers of network services", for which they are not.[84]

36. Also, under Australia's scheme, only "an online location outside Australia" can be blocked.[85] This "important limitation on the power of the Court", wrote Justice Nicholas, "may reflect an assumption that other provisions of the Act provide copyright owners with adequate remedies in respect of online locations situated within Australia".[86] Parliament retained this limit as a rebuttable presumption in Australia's statutory scheme.[87] The narrow US statutory provision also limits blocking to foreign locations.

37. The *de jure* rule in Australia and the US is a *de facto* rule elsewhere. The blocked site in the English test case known as *NewzBin2*, for example, was hosted in Sweden at a domain registered to a Seychelles company.[88] A decision blocking the infamous "Pirate

---

79 *Copyright* Amendment *(Online Infringement) Bill 2015*, (Cth), No 80/2015.
80 *Copyright* Amendment *(Online Infringement) Bill 2018*, (Cth), No 157/2018.
81 Austl, Commonwealth, Senate, *Copyright Amendment (Online Infringement) Bill 2015*, *Revised Explanatory Memorandum*, (2015), ¶6.
82 Federal Court of Australia Act 1976 (Cth), No 156/1976, ss 23, 43.
83 *Copyright Act 1968*, (Cth), No 63/1968, ss 10, 115A; *Telecommunications Act 1997*, No 47/1997, s. 7.
84 *Copyright Act*, ss. 41.25-41.27.
85 *Copyright Act 1968*, (Cth), No 63/1968, s 115A(1).
86 *Roadshow Films Pty Ltd v Telstra Corporation Ltd*, [2016] FCA 1503, ¶38.
87 *Copyright* Amendment *(Online Infringement) Bill 2018*, (Cth), No 157/2018.
88 *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc*, [2011] EWHC 1981 (Ch),

Bay" noted that its operators left the jurisdiction of Swedish (and English) courts, with one said to be in Cambodia operating a Seychelles company.[89] Those findings contrast with the evidence before this Court.[90]

38. In *NewzBin2*, Justice Arnold explained the UK's governing scheme of interwoven legislation, including domestic and European human rights law, and domestic and European intellectual property law.[91] He also noted decades of English and European jurisprudence considering issues related to blocking, concluding: "no uniform approach has emerged among European courts … given that Member States have implemented Article 8(3) of Information Society Directive in different ways".[92] After numerous judgments of the Court of Justice for the European Union (CJEU)[93] that assessment remains fair. Cases from EU member states like Austria, France, Germany, the Netherlands, Spain, Sweden, and elsewhere are, therefore, not particularly helpful to this Court, even if Canada were bound by similar international laws, which it is not.

39. The *obiter dictum* from *Cartier*[94]—speculating that perhaps English courts could or should order blocking even absent a detailed legislative scheme—is, therefore,

---

[*NewzBin2*] ¶58.

89 *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2012] EWHC 268 (Ch), ¶12.

90 The record here shows a contact for the Canadian domain name at apartment complex in Toronto, and includes text messages with a Toronto area (647) phone number: Affidavit of Yves Rémillard, sworn July 15, 2019, ¶¶32, 67 and Exhibits YR-4, YR-39, Shared Appeal Book at volume 4, tab 15, pp 1164, 1410, 1605; Affidavit of Paul Stewart, sworn August 23, 2019, ¶40, Shared Appeal Book at volume 7, tab 29, p 2144; Second Affidavit of Yves Rémillard, sworn September 3, 2019, ¶¶10-11 and Exhibits YR-40 and YR-41, Shared Appeal Book at volume 9, tab 31, pp 2749, 2955, 2757.

91 *NewzBin2*, ¶¶75-91, citing the *Human Rights Act 1998* (UK), c 42; Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No.005 (as amended); European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; *The Electronic Commerce (EC Directive) Regulations 2002*, SI 2002/2013; European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; *Copyright and Related Rights Regulations 2003*, SI 2003/2498; sections 97A and 191A of the *Copyright, Designs, and Patents Act 1988*; European Parliament and Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights; and *The Intellectual Property (Enforcement, etc.) Regulations 2006*, SI 2006/1028.

92 *NewzBin2*, ¶¶92-96, 97.

93 See, for example, *Scarlet Extended SA v Societe Belge des Auteurs Cornpositeurs et Editeurs SCRL (SABAM)*, Case 70/10, [2011] ECR I-11959; *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten v Tele2 Telecommunication GmbH*, Case C-557/07, [2009] ECR I-1227, and *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, Case C-314/12, EU:C:2014:192.

94 *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2016] EWCA Civ 658, [*Cartier*].

inapplicable in Canada. The issue in *Cartier* was whether English courts could order site blocking in the context of trademarks not copyrights. Because the *InfoSoc Directive* pertains specifically to copyright, for trademarks the UK is bound only to implement the *E-Commerce Directive* and *Enforcement Directive*. Lord Justice Kitchen confirmed that English courts had "the obligation" to "adopt a conforming interpretation" of the *Senior Courts Act*.[95] Moreover, experience with blocking in the UK's copyright context—which is distinct from Canada's—enabled the first instance judge in *Cartier* (Justice Arnold) to reach his decision "drawing upon the threshold conditions … under s.97A".[96]

40. The Irish High Court, in a similar situation to Canada's now, was blunt about its inability to order blocking. Justice Charleton, before his elevation to the Supreme Court of Ireland, ruled that he could not follow the High Court of England and Wales on blocking. After lengthy review of relevant statutes, he ruled: "Respecting, as it does, the doctrine of separation of powers and the rule of law, the Court cannot move to grant injunctive relief … even though that relief is merited on the facts."[97] Justice McGovern issued a blocking order in another case only after legislative reform in Ireland.[98] The Irish Court recognized the limits of equitable jurisdiction that it, like Australian and Canadian courts, shares with the UK, and its general remedial powers of injunctive relief.[99]

C.3 Canadian courts should rigorously apply Canada's legal threshold for blocking.

41. Only after statutory thresholds are satisfied should courts examine discretionary factors. The list of factors in *Cartier* actually comes from the detailed recitals of the European statutory scheme for IP enforcement. Necessity, for example, is not only about protecting the plaintiff's rights from irreparable harm (¶¶52-53). In *Cartier*, the Court of Appeal endorsed the High Court's analysis that the *Enforcement Directive* necessitates remedies available under English law include injunctions.[100] The High Court had also explained that human rights can only be restricted where necessary to protect other human rights, in which case a further proportionality analysis is required. In other words, this particular

---

95 *Cartier*, ¶¶56-74; *Marleasing SA v La Comercial Internacional de Alimentacion* SA, C-106/89, [1990] ECR I-4135.
96 *Cartier*, ¶74.
97 *EMI Records (Ireland) Ltd & ors v UPC Communications Ireland Ltd*, [2010] IEHC 377, ¶¶ 134, 138.
98 *EMI Records Ireland Ltd & ors v UPC Communications Ireland Ltd & ors*, [2013] IEHC 274, ¶11.
99 *Supreme Court of Judicature (Ireland) Act 1877*, s.28(8).
100 *Cartier*, ¶¶103-106.

factor is about the necessity of site blocking under inter/supranational copyright and human rights law. Those issues have been debated extensively in the European Parliament, CJEU, and EU national courts.

42. Canadian courts should not take shortcuts around the legal analysis of discretionary factors. *Cartier* ought not be the checklist for blocking orders in Canada without distinctly Canadian legislative, policy, and jurisprudential consideration.

43. In lieu of the factors derived from European directives, Canadian courts should emphasize the core question of proportionality. On one side of proportionality is a spectrum of copyright enforcement options, ranging from less to more intrusive. On the other side are an array of economic impacts, human rights, public interests, internet governance, and technical and policy considerations. The fulcrum between these is the principle of minimal impairment. Less intrusive options should be tried first. The most intrusive option (blocking) should be ordered last.

44. When assessing the spectrum of enforcement options available, citing no evidence that other measures would be effective (¶¶64-65) misplaces the onus and burden of proof. Third parties need not prove other options would be effective. Applicants must prove other options have not been effective. On the other side of the scale, laws protecting freedom of expression and regulating common carriage warrant more than a few comingled sentences (¶97). Policymakers, legislators, and judges around the world have carefully considered each issue under the laws of their particular jurisdiction. The same level of scrutiny should apply in Canada.

PART IV - ORDER SOUGHT

45. CIRA and CIPPIC request that no costs be awarded for or against either intervener.

PARAGRAPHS 1-21 AND 45 ARE RESPECTFULLY SUBMITTED this 3rd day of August, 2020

James Plotkin
Counsel for the Intervener, CIPPIC

Caza Saikaley SRL/LLP
#250-220 Laurier Avenue West
Ottawa, ON K1P 5Z9

Tel: +1 613-564-8271
Fax: +1 613-565-2087
Email: jplotkin@plaideurs.ca

Tamir Israel
Counsel for the Intervener

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tel: +1 613-562-5800 x 2914
Fax: +1 613-562-5417
Email: tisrael@cippic.ca

PARAGRAPHS 1-2 AND 22-45 ARE RESPECTFULLY SUBMITTED this 3rd day of August, 2020

Jeremy de Beer
Counsel for the Intervener, CIRA

Jeremy de Beer Professional Corporation
470 Brierwood Avenue
Ottawa, ON K2A 2H3

Tel: +1 613-263-9081
Email: Jeremy@JeremydeBeer.ca

Bram Abramson
Counsel for the Intervener, CIRA

32M Law Professional Corporation
395 Montrose Ave.
Toronto, ON M6G 3H2

Tel: +1 647-680-8354
Email: bram@32M.io

PART V - AUTHORITIES

Legislation	
1	*An Act respecting The Bell Telephone Company of Canada*, SO 1968, c 48
2	*Bell Canada Special Act*, SC 1967-68, c 48
3	*Canada Post Corporation Act*, RSC 1985, c C-10, https://laws-lois.justice.gc.ca/PDF/C-10.pdf
4	*Canada-United States-Mexico Agreement Implementation Act*, SC 2020, c 1, https://laws-lois.justice.gc.ca/PDF/2020_1.pdf
5	*Copyright Act*, RSC 1985, c C-42, https://laws-lois.justice.gc.ca/PDF/C-42.pdf
6	*Copyright Modernization Act*, SC 2012, c 20, https://laws-lois.justice.gc.ca/PDF/2012_20.pdf
7	*Courts of Justice Act*, RSO 1990, c C.43, https://www.ontario.ca/laws/statute/90c43
8	House of Commons, Legislative Committee on Bill C-11, "Bill C-11: An Act to Amend the Copyright Act", 41st Parliament, 1st Session, Report 1, March 15, 2012, https://www.ourcommons.ca/DocumentViewer/en/41-1/CC11/report-1/
9	House of Commons, Standing Committee on Industry, Science and Technology, "Statutory Review of the Copyright Act", 42nd Parliament, 1st Session, Report 16, June 2019, https://www.ourcommons.ca/Content/Committee/421/INDU/Reports/RP10537003/indurp16/indurp16-e.pdf
10	*Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, SOR/2006-355, https://laws.justice.gc.ca/PDF/SOR-2006-355.pdf
11	*Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives to Promote Competition, Affordability, Consumer Interests and Innovation*, SOR/2019-227, https://laws.justice.gc.ca/PDF/SOR-2019-227.pdf
12	*Telecommunications Act*, SC 1993, c 38, https://laws-lois.justice.gc.ca/PDF/T-3.4.pdf
	| Foreign Legislation
13	*All Writs Act*, codified at 28 USC §1651 (United States), https://www.law.cornell.edu/uscode/text/28/1651
14	Australia, Commonwealth, Senate, *Copyright Amendment (Online Infringement) Bill 2015, Revised Explanatory Memorandum*, (2015), https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5446_ems_87ada78b-8836-421e-bc2f-96cfc19d1f81%22
15	*Copyright Act 1968*, (Australia), https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/ca1968133/

16	*Copyright* Amendment *(Online Infringement) Bill 2015*, (Cth), No 80/2015, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5446_aspassed/toc_pdf/15056b01.pdf
17	*Copyright* Amendment *(Online Infringement) Bill 2018*, (Cth), No 157/2018 (Australia), https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6209_aspassed/toc_pdf/18217b01.pdf;fileType=application%2Fpdf
18	*Digital Millennium Copyright Act*, Pub. L. 105-304, (United States) https://www.congress.gov/105/plaws/publ304/PLAW-105publ304.pdf
19	European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; the Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013, https://data.europa.eu/eli/dir/2000/31/oj
20	European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; Copyright and Related Rights Regulations 2003, SI 2003/2498; sections 97A and 191A of the *Copyright, Designs, and Patents Act 1988*, https://data.europa.eu/eli/dir/2001/29/oj
21	European Parliament and Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights; and Intellectual Property (Enforcement, etc.) Regulations 2006, SI 2006/1028, https://data.europa.eu/eli/dir/2004/48/corrigendum/2004-06-02/oj
22	*Federal Court of Australia Act 1976*, No 156, 1976 (Australia), https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/fcoaa1976249/
23	*Federal Rules of Civil Procedure*, 1938 (United States)
24	*Human Rights Act 1998*, 1998, c 42 (United Kingdom), https://www.legislation.gov.uk/ukpga/1998/42/contents
25	*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*, Bill S 968, 112th Congress, 1st Session, May 26, 2011, (United States), https://www.congress.gov/112/bills/s968/BILLS-112s968rs.pdf
26	*Stop Online Piracy Act*, Bill HR 3261, 112th Cong, 1st Session, October 26, 2011 (United States), https://www.congress.gov/112/bills/hr3261/BILLS-112hr3261ih.pdf|
27	*Supreme Court of Judicature Act (Ireland) 1877*, 1877 c 57 (Ireland), http://www.irishstatutebook.ie/eli/1877/act/57/enacted/en/print
28	*Telecommunications Act 1997*, No 47.1997 (Australia), https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/ta1997214/
29	*United States Copyright Act*, 17 USC 101 *et seq*, https://www.law.cornell.edu/uscode/text/17

	| International Instruments
30	*Agreement Between the United States of America, and the United Mexican States, and Canada*, 30 November 2018, Annex 20-B (Annex to Section J) https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/r2-cusma-20.pdf
31	*Convention for the Protection of Human Rights and Fundamental Freedoms*, November 4, 1950, ETS No 5, 213 UNTS 221, (Council of Europe) https://www.echr.coe.int/Documents/Convention_ENG.pdf
32	*World Intellectual Property Organization Copyright Treaty* (WCT), December 20, 1996 (entered into force 6 March 2002), TRT/WCT/001, 2186 UNTS 121, https://wipolex.wipo.int/en/text/295157
33	*World Intellectual Property Organization Performances and Phonograms Treaty* (WPPT), December 20, 1996, (entered into force 20 May 2002), TRT/WPPT/001, 2186 UNTS 203, http://www.wipo.int/edocs/lexdocs/treaties/en/wppt/trt_wppt_001en.pdf
Jurisprudence	
34	*Apotex Inc v Bayer Inc*, 2018 FCA 32, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/305934/1/document.do
35	*Association canadienne des télécommunications sans fil c Procureure générale du Québec*, 2018 QCCS 3159, https://www.canlii.org/fr/qc/qccs/doc/2018/2018qccs3159/2018qccs3159.html
36	*Bell Canada v Canada (Attorney General)*, 2017 FCA 249, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/303948/1/document.do
37	*Bell Canada v Canada (Attorney General)*, 2019 SCC 66, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/18079/index.do
38	*Bell Canada v Lackman*, 2018 FCA 42, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/306460/1/document.do
39	*Bell Media Inc v GoldTV.Biz*, 2019 FC 1432, https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/424753/1/document.do
40	*Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/18078/1/document.do
41	*CCH Canadian Ltd v Law Society of Upper Canada*, [2004] 1 SCR 339, 2004 SCC 13, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/2125/1/document.do
42	*Crookes v Newton*, [2011] 3 SCR 269, 2011 SCC 47, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/7963/1/document.do
43	*Dominion Telegraph Company v Silver*, (1882) 10 SCR 238, https://scc-csc.lexum.com/scc-csc/scc-csc/en/15264/1/document.do

44	*Electric Despatch Co of Toronto v Bell Telephone Co of Canada*, (1891) 20 SCR 83, https://scc-csc.lexum.com/scc-csc/scc-csc/en/3840/1/document.do
45	*Entertainment Software Assoc v Society Composers*, 2020 FCA 100, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/480092/1/document.do
46	*Equustek Solutions Inc v Jack*, 2014 BCSC 1063, https://www.bccourts.ca/jdb-txt/SC/14/10/2014BCSC1063.htm
47	*Google v Equustek*, [2017] 1 SCR 824, 2017 SCC 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do
48	*Keatley Surveying Ltd v Teranet Inc*, 2019 SCC 43, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/17918/1/document.do
49	*Manitoba v Canadian Copyright Licensing Agency (Access Copyright)*, 2013 FCA 91, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/37749/1/document.do
50	*Microsoft Corporation v 1276916 Ontario Ltd*, 2009 FC 849, https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/57041/1/document.do
51	*Microsoft Corporation v 9038-3746 Quebec Inc*, 2006 FC 1509, https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/53407/index.do
52	Order of Justice LeBlanc, Federal Court File No T-1169-19, July 25, 2019
53	*Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2010-168*, [2012] 3 SCR 489, 2012 SCC 68, https://scc-csc.lexum.com/scc-csc/scc-csc/en/12767/1/document.do
54	*Rogers Communications Inc v Voltage Pictures LLC*, [2018] 2 SCR 643, 2018 SCC 38, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/17254/1/document.do
55	*R v Canadian Broadcasting Corporation*, [2018] 1 SCR 196, 2018 SCC 5, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/16981/1/document.do
56	*R v Sheppard*, [2002] 1 SCR 869, 2002 SCC 26, https://decisions.scc-csc.ca/scc-csc/scc-csc/en/1964/1/document.do
57	*Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers*, [2004] 1 SCR 427, 2004 SCC 45 https://scc-csc.lexum.com/scc-csc/scc-csc/en/2159/1/document.do
58	*Théberge v Galerie d'Art du Petit Champlain Inc*, [2002] 2 SCR 336, 2002 SCC 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/1973/1/document.do
59	*Thomson v Afterlife Network Inc*, 2019 FC 545, https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/405180/1/document.do
60	*Trader v CarGurus*, 2017 ONSC 1841, https://www.canlii.org/en/on/onsc/doc/2017/2017onsc1841/2017onsc1841.pdf

61	*Vancouver International Airport Authority v Public Service Alliance of Canada*, 2010 FCA 158, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/36825/1/document.do
62	*Warman v Fournier*, 2012 FC 803, https://www.canlii.org/en/ca/fct/doc/2012/2012fc803/2012fc803.pdf
	| Foreign Jurisprudence
63	*Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2016] EWCA Civ 658, https://www.bailii.org/ew/cases/EWCA/Civ/2016/658.html
64	Case C-106/89, *Marleasing SA v La Comercial Internacional de Alimentación SA*, [1990] ECR I-4135, (CJEC, 6th Chamber), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61989CJ0106
65	Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, [2009] ECR I-1227, (CJEU, 8th Chamber), http://curia.europa.eu/juris/celex.jsf?celex=62007CO0557&lang1=en&type=TXT&ancre=
66	Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2011] ECR I-11959, (CJEU, 3rd Chamber) http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0070&lang1=en&type=TXT&ancre=
67	Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, EU:C:2014:192, (CJEU, 4th Chamber), http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0314&lang1=en&type=TXT&ancre=
68	*Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2012] EWHC 268 (Ch), https://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html
69	*EMI Records (Ireland) Ltd & Ors v UPC Communications Ireland Ltd*, [2010] IEHC 377, https://www.bailii.org/ie/cases/IEHC/2010/H377.html
70	*EMI Records Ireland Ltd & Ors v UPC Communications Ireland Ltd & Ors*, [2013] IEHC 274, http://www.courts.ie/Judgments.nsf/597645521f07ac9a80256ef30048ca52/ea0a2bbf9271b20380257b9b003b45bd
71	*Roadshow Films Pty Ltd v Telstra Corporation Ltd*, [2016] FCA 1503, https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2016/1503.html
72	*The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors*, [2013] EWHC 2058 (Ch)
73	*Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc*, [2011] EWHC 1981 (Ch), https://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html
Regulatory Decisions	
74	*976 Services—Billing and Collection*, June 26, 1992, Telecom Letter Decision CRTC 92-5, https://crtc.gc.ca/eng/archive/1992/92-5.htm

75	*Asian Television Network International Limited, on behalf of the FairPlay Coalition—Application to Disable Online Access to Piracy Websites*, Telecom Decision CRTC 2018-384, CRTC File No: 8663-A182-201800467, October 2, 2018, https://crtc.gc.ca/eng/archive/2018/2018-384.pdf
76	*Decision re application of Richard Warman*, Telecom Commission Letter, CRTC File No: 8622-P49-200610510, August 24, 2006, https://crtc.gc.ca/eng/archive/2006/lt060824.htm
77	*Public Interest Advocacy Centre—Application for Relief Regarding Section 12 of the Quebec Budget Act*, Telecom Decision CRTC 2016-479, CRTC File No: 8663-P8-201607186, December 9, 2016, https://crtc.gc.ca/eng/archive/2016/2016-479.pdf
78	*Review of Internet Management Practices of Internet Service Providers*, Telecom Regulatory Policy CRTC 2009-657, October 21, 2009, CRTC File No: 8646-C12-200815400, https://crtc.gc.ca/eng/archive/2009/2009-657.pdf
Secondary Materials	
79	Canadian Music Publishers Association, C-11 Submission, November 29, 2011, https://www.ourcommons.ca/Content/Committee/411/CC11/WebDoc/WD5459877/411_C11_Copyright_Briefs/CanadianMusicPublishersAssociationE.pdf
80	Canadian Radio-television and Telecommunications Commission, Policy Development and Research, "Navigating Convergence: Charting Canadian Communications Change and Regulatory Implications", February 2010, https://crtc.gc.ca/eng/publications/reports/rp1002.pdf
81	Law Commission of Ontario, "Defamation Law in the Internet Age", March 2020, https://www.lco-cdo.org/wp-content/uploads/2020/03/Defamation-Final-Report-Eng-FINAL-1.pdf
82	Testimony of Catharine Saxberg, Executive Director, Canadian Music Publishers Association, C-11 Committee, House of Commons Legislative Committee on Bill C-11, 41st Parliament, 1 Session, March 6, 2012, https://www.ourcommons.ca/Content/Committee/411/CC11/Evidence/EV5429125/CC11EV08-E.PDF
83	Testimony of Craig McTaggart, Director, Broadband Policy, TELUS, House of Commons Legislative Committee on Bill C-32, 40th Parliament, 3rd Session, March 22, 2011, https://www.ourcommons.ca/Content/Committee/403/CC32/Evidence/EV5057232/CC32EV19-E.PDF
84	United States, *Hearing on Approaches to Foreign Jurisdictions to Copyright Law and Internet Piracy Before the US Senate Committee on the Judiciary*, 116th Cong, 10 March 2020 (Stanford K. McCoy), https://www.judiciary.senate.gov/imo/media/doc/McCoy%20Testimony.pdf

Court File No. A-440-19

TEKSAVVY SOLUTIONS INC (Appellants)	AND	BELL MEDIA INC AND OTHERS (Respondents)	AND	CANADIAN INTERNET REGISTRATION AUTHORITY AND OTHERS (Interveners)

FEDERAL COURT OF APPEAL

MEMORANDUM OF FACT AND LAW OF THE INTERVENERS, THE CANADIAN INTERNET REGISTRATION AUTHORITY AND THE SAMEULSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC

Jeremy de Beer Professional Corporation
470 Brierwood Avenue
Ottawa, ON K2A 2H3

Jeremy de Beer
(Jeremy@JeremydeBeer.c)

Tel: +1 613-263-9081

Counsel for the Intervener, CIRA

32M Law Professional Corporation
395 Montrose Ave.
Toronto, ON M6G 3H2

Bram Abramson
(bram@32M.io)

Tel: +1 647-680-8354

Counsel for the Intervener, CIRA

Caza Saikaley SRL/LLP
#250-220 Laurier Avenue West
Ottawa, ON K1P 5Z9

Alyssa Tomkins
(atomkins@plaideurs.ca)
James Plotkin
(jplotkin@plaideurs.ca)

Tel: +1 613-565-2292
Fax: +1 613-565-2087

Counsel for the Intervener, CIPPIC

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tamir Israel (tisrael@cippic.ca)

Tel: +1 613-562-5800 ext 2914
Fax: +1 613-562-5417

Counsel for the Intervener, CIPPIC

APPENDIX E

Submission to the Broadcasting and Telecommunications Legislative Review Panel

January 11, 2019

About CIRA

1. The Canadian Internet Registration Authority (CIRA) welcomes the opportunity to provide comments to the Broadcasting and Telecommunications Legislative Review. CIRA is the member based not-for-profit organization best known for managing the .CA top level domain on behalf of all Canadians, developing and implementing policies that support Canada's internet community, and representing the .CA registry internationally.

2. CIRA's core role is ensuring the stability and security of the .CA top-level domain registry and the underlying domain name system technologies that support the accessibility of every .CA domain. Related to this role, CIRA also provides cybersecurity services such as a DNS anycast service, for which we operate networks and equipment in Canada and on five continents internationally, and a DNS monitoring tool, which enables network operators, businesses and Canadians to protect their networks.

3. CIRA takes pride in being one of the many thousands of organizations that ensure the global internet functions on a daily basis, while playing a unique role in Canada's internet ecosystem. It is with this technical understanding of how the internet functions, as well as our long-time involvement in domestic and international issues related to the governance of the internet that CIRA offers the following comments.

Introduction

4. As internet infrastructure increasingly serves as the delivery mechanism for culture, commerce and communications, governments everywhere are grappling with challenges brought about by the digital age. These challenges include:

    - how to protect user privacy,
    - how to exercise oversight of content distribution to address a range of issues, including cultural policy objectives, copyright infringement, hate speech and fake news,
    - growing concerns about cybersecurity and how to protect against attacks,
    - issues of jurisdiction on a global network,
    - and how to uphold the spirit of the internet envisioned by its founders amidst these concerns.

5. We have reached an inflection point where the internet is seen as not only a bastion of progress, but also a challenge to long-held government policy objectives. The paradigm shift is evident in recent battles fought by policymakers around the world. In the United States these battles have taken the form of the repeal of net neutrality and the failed Stop Online Piracy Act

(SOPA). In the European Union, the challenges are evident in the controversial Copyright Directive and the recently implemented General Data Protection Regulation (GDPR).

6. Canada faces many of the same challenges. It is increasingly clear that the internet is not a direct analogue for the publishers, broadcasters or even the telephone companies of the past. In order to contend with the above named concerns today and into the future, Canada's communications legislation requires updates. CIRA's comments will focus on three issues we believe are important for ensuring the continued power of the internet to unleash innovation and creativity. First, we will address the hazards of treating the internet and the broadcast system as equivalent entities. Next, we discuss Canadian content in the digital age. Finally, we examine the need to recognize emerging players and the evolving architecture of the content distribution landscape.

The internet is more than a content delivery system

7. The telecommunications system is a general-purpose conduit for many forms of communications, but it is not a form of communication in and of itself. The internet, in particular, serves as the transportation system for many "applications" including telephony, file transfers, email, streaming audio and video, graphics and the written word, to name a few. It is important to distinguish between the internet and the applications delivered over it.

8. The user situated at the end-point of a network defines which types of communications they access and the device they choose to access them on. The user's ability to freely define which applications are used at the end-point is known as the end-to-end principle. This allows many different systems to interconnect and interoperate. The end-to-end principle is a precursor to the principle of net neutrality and the decentralization it brought about in packet-switched networks represented a major departure from the centralized architecture of traditional telephony networks. With the internet, the intelligence of the network is primarily located at the end-points, with end-users.

9. A helpful reference model for understanding the functions of communications infrastructure is the Open System Interconnections (OSI) model, or OSI stack. [1] The seven layer model (Figure 1) was developed by the International Standards Organization (ISO) in the 1980s and standardizes the functions of the different layers of communications and computing systems. The reference model describes the conceptual division of tasks on a network and facilitates the interoperability of many communications systems, including the internet.

[1] ISO/IEC 7498-1:1994, Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. International Organization for Standards, 1994.

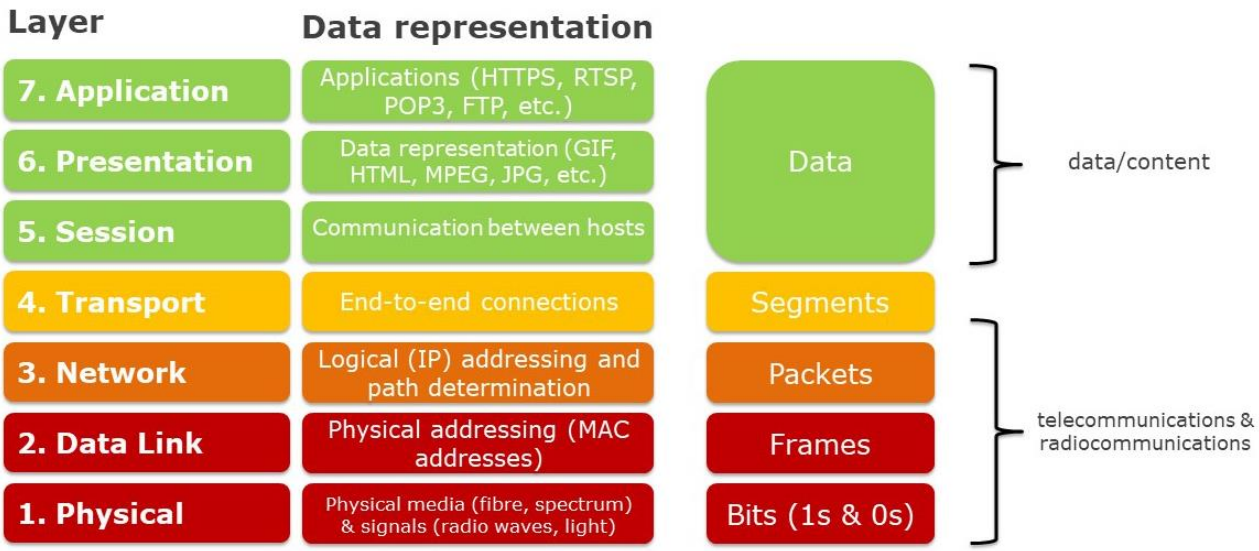


Figure 1: The Open Systems Interconnection (OSI) model

10. Communications law in the digital age should attempt to regulate at the layers associated with its policy objectives. The bottom 3 layers of the OSI model (the physical, data link, and network layers) constitute basic, network-specific functions. This is the realm of telecommunications, which the *Telecommunications Act* defines as "the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system." [2] The upper layers of the OSI model perform application specific functions.

11. The upper layers are more closely associated with the realm of broadcasting or content distribution. The *Broadcasting Act* defines broadcasting as, "any transmission of programs, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of broadcasting receiving apparatus, but does not include any such transmission of programs that is made solely for performance or display in a public place." Telecommunications network operators are not responsible for initiating the transmission or reception of programming on the internet. This is the role of over-the-top service providers. Internet service providers (ISPs) merely carry the signal once a transmission is initiated.

12. The relationship between telecommunications and content distribution has caused some to conclude the internet is synonymous with the broadcast system and that it ought to be treated as such for regulatory purposes. However, the intentions behind telecommunications law and broadcasting law are fundamentally different. The *Telecommunications Act* exists to facilitate competitive market outcomes and the development of a robust communications system.[3] The *Broadcasting Act*, on the other hand, is a vehicle for cultural policy and Canadian identity with

[2] Telecommunications Act (S.C. 1993 c.38) ss 1, *Definitions.*
[3] Telecommunications Act (S.C. 1993, c. 38) ss 7, *Objectives.*

the objectives of reflecting Canadian society and strengthening the production and consumption of Canadian programming.[4]

13. While programming prepared for conventional broadcasting distribution is also delivered online, that does not mean online delivery of this programming is "broadcasting." An approach that blends broadcasting and telecommunications legislation because Canadians access television programs and radio on the internet is analogous to combining the *Bank Act* and the *Telecom Act* because Canadians bank online. The internet is a delivery platform for a diverse array of activities, with audio-visual content being only one of them.

14. According to CIRA's primary research, 39% of Canadians watch movies, television, and other videos online. We also found that 32% of Canadians access music and podcasts on the internet. However, Canadians also engage in a wide variety of other online activities. In 2018, more Canadians said they use the web to shop (52%), access the news (55%), bank (73%), engage on social media (61%), and send email (89%) than those who said they watch video or listen to audio content.[5]

15. This joint review of legislation seeks to accomplish two difficult and possibly conflicting priorities. The first is determining how to continue funding Canadian content creation in the globally interconnected digital economy. The second is achieving universal access to high quality, affordable broadband. In pursuit of the first goal, some have proposed that internet service providers ought to contribute to Canadian content creation. However, internet service providers already face many challenges related to ensuring all Canadians, including those in rural, remote and Indigenous communities, have access to high quality, affordable broadband.

16. Any move toward a regulatory framework that could link broadcasting policy to the price of an internet connection would be a step in the wrong direction and could lead to higher consumer costs. The internet is a general-purpose telecommunications service, which remains prohibitively expensive in some rural and remote locations. Canadians rely heavily upon their internet connections for a variety of day-to-day tasks. They access banking, shopping and e-mail in greater numbers than streaming audio and video. Streaming audio and video is only one of many activities Canadians engage in online. As a result, we should not view the internet through the prism of the broadcasting industry.

Canadian content in the digital age

17. CIRA's 2018 Internet Factbook research identified Canadians' appetite for home-grown content. Of respondents who use a home internet connection to access audio or video, 58% said they actively seek out Canadian programming at least occasionally. As the stewards of the .CA country code top-level domain, CIRA understands the importance of asserting Canadian identity

[4] Broadcasting Act (S.C. 1991, c. 11) ss 3, *Declaration.*
[5] Canada's Internet Factbook 2018, Canadian Internet Registration Authority (CIRA), June 13, 2018.

and maintaining relevance online. CIRA marketing encourages Canadians to "Choose Canada. Choose .CA," and they are. The market share of .CA domain names in Canada grew from 25% in 2009 to 33% in 2018. Market share for .COM dropped from 59% to 54% in the same period. Canadians are increasingly choosing .CA to represent their brands and personal presence online. It is against this backdrop that we recommend the objectives of broadcasting policy should emphasize discoverability, amplification, and recognition of Canadian content distributed via the internet.

18. There are technical challenges and repercussions associated with the 20th century tools of broadcasting regulation that must not enter the telecommunications system. In pursuit of cultural objectives, the *Broadcasting Act* has been leveraged to limit foreign television channels that compete with Canadian channels. Broadcasting policy has also required broadcasting distribution undertakings (BDUs) to grant priority carriage to Canadian TV stations and to offer a majority of Canadian channels. These measures, if implemented on the internet, would take the form of content blocking, bandwidth throttling[6] or granting priority carriage to Canadian programming. Any of these would undermine the principles of net neutrality.

19. Fortunately, the language of net neutrality is already present in section 27 of the *Telecommunications Act*, which prevents undue preference and discriminatory rates, and in section 36, which prohibits influencing the meaning of communications. It is this legislation that empowered the CRTC to develop the internet traffic management practices (ITMP) policy framework. This framework forms the basis of Canada's net neutrality regulations. These century old principles of common carriage are not technology specific, but the concepts continue to serve us well in the digital age. However, the window is open to strengthen the language and explicitly enshrine net neutrality in law rather than as a matter of regulatory policy. Given the rapidly changing nature of internet architecture, we caution against any language that is overly technology-specific.

20. The tools of the *Broadcasting Act,* however, include preferential treatment for Canadian programming. This is diametrically opposed to the concept of an 'open internet.' CIRA submitted views on the issue of blocking in response to the 2018 *FairPlay Coalition Application to disable online access to piracy websites.*[7] CIRA does not see limiting the openness of the internet as sacrosanct, but as a measure that should only be permitted in exceptional circumstances such as in cases of child abuse and infrastructure abuse (e.g. distribution of malware, denial of service attacks). Preferential treatment of Canadian programming would not qualify as one of these exceptions.

[6] According to Wikipedia, "*bandwidth throttling* is the intentional slowing or speeding of an internet service by and internet service provider."

[7] Intervention of the Canadian Internet Registration Authority in CRTC Public process 2018-0046-7 Asian Television Network International Limited application on behalf of itself and a number of other persons (collectively, FairPlay Canada) on website blocking.

21. Furthermore, any bid to apply the tools of 20th century broadcasting regulation would fail on a technical level. Efforts to block or limit access are generally ineffective and users who discover blocking have many options to defeat or circumvent it. Even average users can circumvent blocking with moderate technical skills and knowledge. We also know that blocking tends to cause collateral damage. Interception and alteration of IP addresses or DNS responses leads to problems that take other valid services offline.

22. On the other end of the spectrum, blocking – particularly IP address blocking – can have limited effectiveness when applied to large service providers whose content is hosted across multiple data centers or in a Content Delivery Network whose IP addressing schemes are highly distributed and dynamic. In this casetheir IP addresses change all the time by virtue of their network architecture. It is for reasons like this that regulating audio-visual content on the internet is a losing battle.

Emerging issues in networking and content distribution

23. As a result of consumer demand for content, including streaming video and audio, over-the-top service providers are building private networks to improve service performance for users. These content delivery networks (CDNs) are changing global internet infrastructure. The purpose of content delivery networks is to store content, including web pages, advertisements, videos, pictures and audio, as physically close to the end user as possible. Shortening the physical path between the user at the "edge" and the servers where content is stored results in a faster, more responsive online experience. Milliseconds of performance matter. When a Toronto user accesses a Youtube video, the request is likely served by a content cache located in Toronto rather than a data centre in California.

24. In order to serve customers around the globe, CDNs distribute copies of frequently accessed files to servers located in geographically strategic locations. These are often major population centres with high concentrations of internet users, colloquially known as "eyeballs." As a result, the CDN does not need to pay an upstream Tier 2 or Tier 1 network each time a customer accesses a video, webpage or photograph. Instead, the CDN optimizes bandwidth usage by pushing and caching content on a global network of servers according to a schedule.

25. These servers or caches are often located in partnership with local access ISPs or at an internet exchange point (IXP). An IXP is a hub where independent networks can interconnect directly to one another, providing high-bandwidth and low-latency access at a lower cost than traditional transit.[8]

[8] Canada's Internet Infrastructure: Made-in-Canada Internet Exchange Points (IXPs), Canadian Internet Registration Authority (CIRA).

26. In addition to locating thousands of servers around the globe, CDNs are investing in submarine cables to move content across oceans.[9] This reduces the requirement to pay a Tier 1 transit ISP to move packets between continents.

27. Content delivery network operators include household names of major online service providers like Facebook, Google, Netflix, Microsoft and Apple. Any major enterprise with a global online presence generally operates a CDN. CDNs are also run by companies such as Akamai, Cloudflare, Fastly, and Limelight. These lesser-known entities are responsible for delivering a significant proportion of internet traffic. They operate by aggregating the needs of many web properties in order to serve their content locally. News websites, for example, may hire a CDN to replicate and store their content in major local markets around the world.

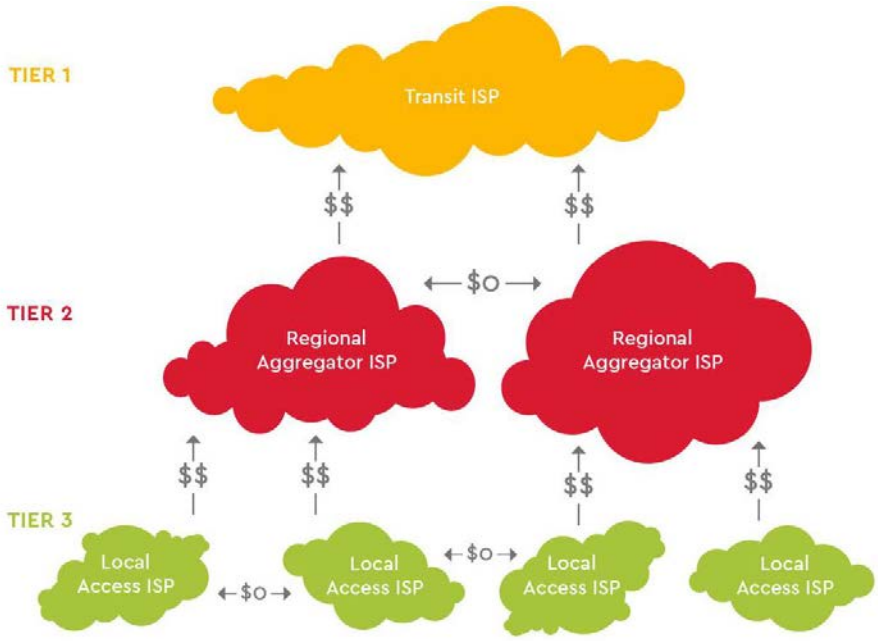


Figure 2: Old internet architecture

28. Content delivery networks are not only altering the architecture of the global internet, but also the flow of capital. In traditional global internet architecture, payments flow upstream from Tier 3 local access ISPs to Tier 2 traffic aggregators with regional footprints. From there, Tier 2 networks pay Tier 1 transit networks with global footprints. Transit networks move traffic internationally (Figure 1). There are less than a handful of Tier 1 networks with truly global footprints. Tier 1 networks have historically been the owners of submarine cables used for transmitting terabytes of data across oceans.

[9] Optical Illusions: Content Providers and the Impending Transformation of International Transport, Tim Strong, Telegeography. Presentation to the North American Network Operators Group (NANOG). October 4, 2017.

29. Networks with similar traffic loads exchange traffic on a $0, or settlement free basis. Tier 3 networks may exchange traffic directly with each other for free, but are required to pay an upstream network to move packets further afield. Likewise, the Tier 1 and 2 networks exchange traffic with their peers. Content delivery networks are disrupting this model. CDNs locate their files as close to the user as possible, often at the edge of Tier 3 local access networks. This new architecture sees a high proportion of internet traffic skipping Tier 1 and Tier 2 networks, reaching consumers directly via their local access networks. According to Cisco, 72 percent of all global internet traffic will cross CDNs by 2022, up from 56 percent in 2017.[10]

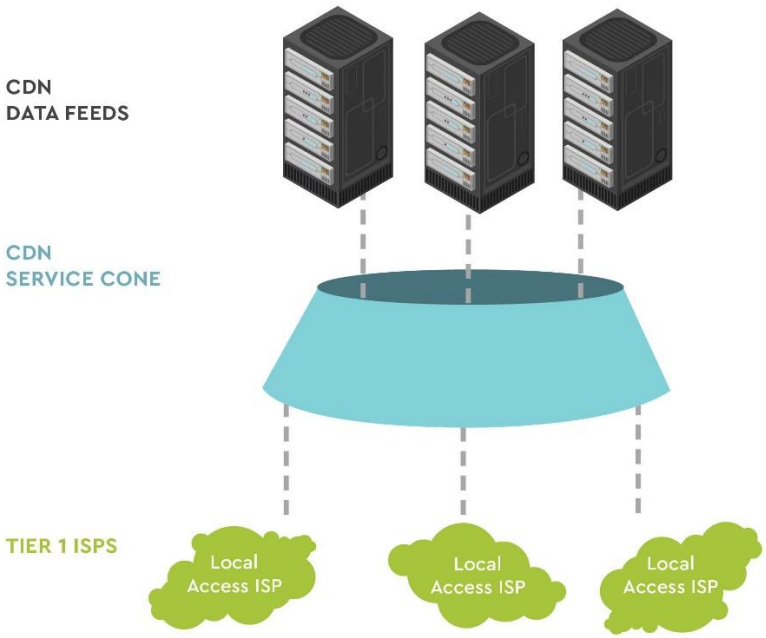


Figure 3: New internet architecture

30. For the purposes of this legislative review, it is worth noting that content delivery networks are dominant players in the internet ecosystem. Their service territories are global and their networks are unregulated by both telecommunications and broadcasting law. This is not to say that these private networks ought to be regulated under telecommunications legislation. There is no apparent market failure. In fact, the content delivery market is competitive for both enterprise and aggregator CDNs. Additionally, their efforts to locate content close to the network's edge contribute to a better quality of service and therefore a better online experience for Canadian consumers. Furthermore, when Tier 1 ISPs interconnect directly with CDNs, it

[10] Cisco Visual Networking Index: Forecast and Trends, 2017–2022, Tables 9 and 16. Global content delivery network internet traffic, 2017-2022. November 26, 2018.

reduces their costs for upstream internet transit, theoretically leading to cost savings for their downstream customers: Canadian internet users.

31. However, we point out that CDNs have caused major changes to internet architecture because the rate of change in the communications sector continues to be rapid. Any legislative updates must be flexible enough to take rapid technological change into account and must not create an environment that limits innovation or creativity in the sector.

Conclusion

32. The internet is a general-purpose, neutral conduit over which many applications run. It is imperative that we distinguish clearly between the applications that run on top of the internet, and the internet itself. While bandwidth intensive, audio-visual constitutes only a small portion of the applications Canadians access over the internet therefore broadcasting interests must not be permitted to steer telecommunications legislation. Instead, broadcasting should be regulated separately and any new policy or legislative approaches should emphasize discoverability, amplification and recognition of Canadian content that is distributed via the internet. Finally, amidst this review, it is important to consider that the rate of change continues to be rapid and that any legislative updates must be flexible enough to account for continued technological change.

*******END OF SUBMISSION*******

APPENDIX F

CANADIAN INTERNET REGISTRATION AUTHORITY INTERVENTION

Re: Public process number: 2018-0046-7 Asian Television Network International Limited application on behalf of itself and a number of other persons (collectively, FairPlay Canada) on website blocking.

1. The Canadian Internet Registration Authority (CIRA), welcomes the opportunity to comment on the FairPlay Canada Proposal. CIRA is a member-based not-for-profit organization, best known for managing the .CA internet domain on behalf of all Canadians, developing and implementing policies that support Canada's internet community, and representing the .CA registry internationally.

2. CIRA's core mandate is to ensure the safety and security of the .CA domain, including its DNS, registry and other related underlying technologies. Related to this role, CIRA also provides cybersecurity services such as a DNS anycast product, for which we operate networks and equipment across Canada and on five continents internationally. More recently, CIRA also launched a DNS monitoring tool, which enables network operators, businesses and Canadians to protect their networks at the DNS level.

3. CIRA takes pride in being one of the many thousands of organizations that help the global internet to function on a daily basis, while playing a unique role in Canada's internet ecosystem. It is with this technical understanding of how the internet actually works, as well as its long-time involvement in domestic and international issues related to the governance of the internet, that CIRA offers the following comments.

Need to keep the internet open

4. It goes without saying that the FairPlay proposal is diametrically opposed to the concept of an 'open internet' for which CIRA has long stood. The openness of the internet is not a vague concept but rather goes to the very heart of its existence and how it came to be. To quote James Mwangi, in the Foreword to the March 2014 Dalberg Global Development Advisors report "Open for Business? The Economic Impact of Internet Openness":

> *"We take the capabilities of today's internet for granted, as though it was inevitable it would evolve in this way. But in the early days of the internet, few people knew how profoundly this*

technology could transform our lives. We've witnessed growth that would have been impossible to predict, growth that can only be understood in the context of one essential attribute of the system: the openness of the network. Since its emergence, the internet has remained an open platform, allowing any of us to innovate, create new services and tools, share freely and widely, and access all of the products and services that others have made available…Without openness, many of the services and tools we rely on in our daily lives would not be possible."

5. In a recent paper, the Internet Society builds on this to say that:

"…in the internet, openness is about opportunity, not ideology: it is about the opportunity for students, entrepreneurs, creators, and inventors to explore, try and test new ideas and new business models without asking permission from any established gatekeeper. Openness is not about promoting the social or political values of one group over others. It is freedom, not disorder. The open internet enables an environment of social and economic growth and empowerment not because its supporters relentlessly assert "openness is good," but because openness confers extraordinary tangible benefits that would otherwise be difficult or impossible to obtain:

- *As a tangible network infrastructure composed of hosts, routers, service providers, protocols, and many other technical components, the internet is optimized for interoperability—peer components interact with each other without extensive prior configuration because information is shared openly, and every developer and operator has open access to the externally visible behavior of each element of the internet system.*
- *As an operational infrastructure that relies on the voluntary participation of many different parties to manage its independent parts, the internet is an open society of individuals and organizations that fulfill their separate local missions by collaborating to make the global internet work.*
- *As an innovation engine that supports the development of new technical standards and policy initiatives, the internet succeeds because openness, in terms of transparency, access, and participation, brings the best ideas to the table, distributes them widely, and engages everyone in the*

process of turning them into new services and applications that enhance the quality of life in all corners of the world."[1]

6. It is with this commitment, indeed bias, to an open internet that CIRA has reviewed the debate around the FairPlay proposal. CIRA does not see limiting the openness of the internet as sacrosanct, but rather as something that should only be permitted in exceptional circumstances where limiting internet openness can be justified, such as in cases of child pornography and infrastructure abuse (e.g. distribution of malware, denial of service attacks). For CIRA, the central question is whether the proposed limitations on internet openness proposed by FairPlay can be justified in these circumstances.

Challenges of the FairPlay Proposal

Copyright infringement and enforcement

7. CIRA has carefully reviewed the FairPlay proposal as well as virtually all of the commentary that has been published to date, in particular the criticisms from Michael Geist of the University of Ottawa, who is an elected CIRA Board Director, as well as commentary from the Internet Society Canada Chapter. CIRA supports statements that Prof. Geist and the ISCC make in their interventions regarding copyright infringements and enforcement, in particular that:

    - The problem of piracy has been exaggerated;
    - To the extent that piracy exists, it is having little impact on the production of domestic digital and television production;
    - The proposed regime is not in line with those operating in other countries; and,
    - Existing tools and remedies using the Copyright Act are both effective and sufficient.

8. CIRA strongly supports statements from Minister Navdeep Bains, who, having responsibility for both the Copyright Act and the Telecommunications Act, has said:

    "We understand that there are groups, including Bell, calling for additional tools to better fight piracy, particularly in the digital domain. Canada's copyright system has numerous legal provisions and tools to help copyright owners protect their intellectual property, both online and in the physical realm. We are committed

[1] *What Do You Mean When You Say 'Open Internet'?,* by Sally Shipman Wentworth, Vice President Global Policy Development, the Internet Society, Sept. 4, 2014. Retrieved on March 20, 2018

to maintaining one of the best intellectual property and copyright frameworks in the world to support creativity and innovation to the benefit of artists, creators, consumers and all Canadians."

9. Additional arguments related to copyright enforcement legislation, jurisdiction and policy are covered in depth by other interventions.

Technical Comments Related to the Proposal

10. Given its technical expertise, CIRA will focus its intervention on the technical implications and consequences of 'website blocking.'

Technical introduction

11. The FairPlay Canada proposal does not provide an explanation about what technical mechanism(s) the ISPs would employ, or be allowed to employ, in order to implement the proposed Independent Piracy Review Committee's (IPRC) recommendations. As the operator of Canada's top-level internet domain, CIRA is obviously concerned that pressure will be put on registries to get involved in addressing suspected .CA piracy sites.

12. Given that there are only a few sensible places to block traffic on the internet, CIRA is focusing on the challenges related to the most likely solutions ISPs would undertake were they to be directed to filter and block specific websites. While the concept of filtering can be applied to many points within a network – and thereby many points within the internet – CIRA will restrict its analysis with a few basic assumptions, as follows:
    i. This would be enacted without the co-operation of Canadian internet users. That is to say it would not be filtered in the home, at work, or at the firewall, router or modem of the user.
    ii. It would be wholly undertaken by the ISPs and would require some sort of coordination, in order to ensure as much coverage as possible in Canada.
    iii. The blocking would use a shared "blacklist" or domain names and IP addresses that would be given to the ISPs by the IPRC

13. In short, the blocking intervention would be taken somewhere within the end-to-end communication path between the user and the website containing potentially pirated content.

14. Within that path there are three (3) components in delivering internet content as defined by the Internet Engineering Task Force (IETF)[2]. They are:

[2] IETF, Internet Architecture Board, RFC 7754, Sec. 3.4. "Components Used for Blocking"

1. **Endpoints**: The actual content of the service is typically an application-layer protocol between two or more Internet hosts. In many protocols, there are two endpoints, a client and a server.
2. **Network services**: The endpoints communicate by way of a collection of IP networks that use routing protocols to determine how to deliver packets between the endpoints.
3. **Rendezvous services**: Service endpoints are typically identified by identifiers that are more "human-friendly" than IP addresses. Rendezvous services allow one endpoint to figure out how to contact another endpoint based on an identifier. An example of a rendezvous service is the domain name system. Distributed Hash Tables (DHTs) have also been used as rendezvous services.

15. Additionally, as defined by the Internet Society, there are five (5) categories of blocking[3] that could be reasonably undertaken:

    - IP/Protocol-based blocking.
    - Deep Packet Inspection-based blocking.
    - URL-based blocking.
    - Platform-based blocking (especially search engines).
    - DNS-based blocking.

16. For the purposes of this submission, CIRA will restrict its comments to **Network Services** and **Rendezvous Points** (specifically Domain Names) within the categories of **IP/Protocol Blocking** and **DNS-based Blocking** as they are the approaches taken most often in other jurisdictions. Additionally, these approaches share similar challenges in terms of raising open internet issues.

Technical challenges

17. There is common and commercially available software available for blocking using the above-mentioned techniques. They come in a variety of forms (firewall products, 3rd party products, appliances, etc.) which block internet traffic to a specific address, IP, URL/URI or even within the DNS itself.

18. This can be an effective management tool if used with the knowledge and permission of the users, for example when deployed by a school board to prevent students from visiting websites known to host harmful content such as viruses and malware, or containing inappropriate or offensive material. In these cases, blocking must be inserted somewhere within **Network Services** or **Rendezvous Points** and not at a client **endpoint**. The user, for example

[3] The Internet Society, Internet Society Perspectives on Internet Content Blocking: An Overview, Overview of Content Blocking Techniques

the school administration, needs to be aware and agree to allow a single access control point somewhere along the network path.

19. There is a further distinction with awareness and cooperation related to the user endpoint, whether it is software installed on the client machine, in-browser functionality or built in to the access hardware (the modem and/or router). The distinction is that an informed and cooperative user is preventing infiltration and is acquiescing to this blocking for protection. Without awareness and consent, the user is being unwittingly "ring-fenced" as to which content the can and cannot be accessed.

20. As we assume that Canadian internet users are not giving permission to IPRC or the ISPs to block traffic using this set of methods, the effectiveness of this approach is compromised. Set out below are the most obvious drawbacks to enacting blocking without the permission or knowledge of the end user.

    i. First, any user discovering this type of blocking has many options to defeat or circumvent it. Using VPNs, TOR or other obfuscated or encrypted end-to-end technology, even average users could circumvent this blocking with only moderate technical skills and knowledge.[4] There are many resources available: YouTube tutorials, commercial "defeat" products and systems, and freely shared information from a variety of experts making end-user circumventing straightforward and easy. There are also large-scale infrastructures dedicated to defeating blocking, such as the TOR Network. This "other" endpoint, whomever they might be, is unlikely to cooperate with IPRC and Canadian ISPs engaged in blocking. Without co-operation from either endpoint, there are many paths that the data can take around any blocking put in place, significantly negating the success of the blocking approaches mentioned above.

    ii. Second, this approach is also ineffective against content delivery networks (CDNs) as they dynamically change IP addresses[5] and/or have an Anycast architecture.[6] As these IP addresses are, effectively, in the middle of the network path, IP blocking has a significant risk of affecting more than just the intended target. Similarly, more sophisticated individual providers can change IPs easily; this would set up a cat-and-mouse scenario witnessed with The Pirate Bay.[7]

[4] PC Magazine, How to Hide Your IP Address
[5] Cloudflare, Dynamic DNS
[6] Cloudflare, What is Anycast?
[7] CurrentlyDown.com, Is the Pirate Bay down?

iii. Third, using blocking within **Network Services** and **Rendezvous Points** is a blunt instrument, akin to using a hammer to kill a fly. Both over-blocking and under-blocking are significant risks to any blocking regime[8].

> *"This type of over blocking also occurred in India. The Ministry of Communications & Information Technology in India ordered ISPs to block access to a specific Yahoo! Group named kynhun. The ISPs were unable to block the specific URL, presumably due to a lack of specialized technology, so instead they blocked access to the entire groups.yahoo.com domain by configuring their routers to block access to the specific Yahoo! Groups IP address. This caused many thousands of Yahoo! Groups to be inaccessible to internet users in India"*

iv. Finally, there are unintended consequences of blocking using these techniques. For example, a small business' website could be unintentionally infected with distribution software. If its ISP blocks this site at either the DNS or in certain instances at the IP, the user's email (using the domain name of the blocked website) could stop working, having an impact on that business' ability to maintain daily operations – an unintended consequence of blocking. Further complicating this approach is that in this scenario, the small business would see its online presence shuttered, without being given a reason, nor receiving assistance on how to rectify the situation. There are many examples of overblocking, as evidence in Andrew McDiarmid's work[9].

Conclusion

21. There are a myriad of challenges associated with the FairPlay proposal:
    i. Ability to defeat and circumvent;
    ii. Ineffectiveness in key circumstances; and,
    iii. Unintended consequences.

22. At the outset, we posited that for CIRA, the central question is whether the proposed limitations on internet openness proposed by FairPlay can be justified in these circumstances that they seek to remedy. By this measure, we find the proposal wholly lacking and therefore oppose it steadfastly.

[8] University of Illinois at Chicago First Monday, N. Villeneuve et al, The Filtering Matrix: Unintended Consequences
[9] McDiarmid, Andrew, Center for Democracy & Technology (CDT), An Object Lesson in Overblocking

APPENDIX G

Request for Disclosure of Registrant Information - Rules and Procedures
Version 1.7 (May 20, 2015)

Background

These Rules and Procedures are implemented pursuant to CIRA's *Privacy Policy*, to provide the process for certain persons to request the disclosure, under certain limited and specified circumstances, of certain specific information of Registrants that is not publicly available through CIRA's WHOIS search tool.

Except as expressly specified herein or in the Policy, any other request for disclosure of information of Registrants must be by way of an order, ruling, decision, subpoena, warrant, or judgment.

These Rules and Procedures outline:

- What specific information of Registrants may be disclosed under these Rules and Procedures, pursuant to a request for disclosure;
- Who may request such information be disclosed by CIRA, pursuant to these Rules and Procedures ("Requestors"); and
- What express requirements the Requestors must meet, before CIRA will consider disclosure of information, pursuant to a request.

All capitalized terms used herein but not defined, shall have the meanings as set out in CIRA's *Registrant Agreement* or *Registrar Agreement*.

Rules and Procedures

1. Information Subject to Disclosure.

   These Rules and Procedures provide for the potential disclosure of the following information of Registrants, as found in the CIRA Registry:

   a. The name of the Registrant;
   b. The postal address and email address of the Registrant (if available);
   c. The name of the Registrant's Administrative Contact and Technical Contact; and
   d. The postal address and email address of the Registrant's Administrative Contact and Technical Contact;

   (collectively, "Information").

   CIRA will not disclose any other information under these Rules and Procedures.

2. Who May Request Disclosure of Information. Requestors must be a person who complies with all of the obligations of Section 3 below.

3. Requirements. To be able to request Information, a Requestor must meet **all** of the following requirements:

a) The Information is not publicly available through CIRA's WHOIS search tool.

b) The Requestor must have a current, good faith Dispute with a Registrant. For purposes of these Rules and Procedures, "Dispute" means that a Requestor reasonably believes in good faith that a Registrant's domain name and/or its content:
   i. infringes Requestor's Canadian: (i) registered trademark, (ii) registered copyright, or (iii) issued patent;
   ii. infringes Requestor's Canadian registered (Federal or Provincial) corporate, business or trade name; or
   iii. is making use of the Requester's personal information without their knowledge or consent to pass off as or impersonate them in order to commit a crime (such as fraud, theft or forgery), to procure money, credit, loans, goods or services without authorization. (Identity Theft)

   Nothing else shall constitute a Dispute hereunder.

c) The Requestor or their authorized representative must provide such supporting documentation regarding the applicable Dispute as may be required by CIRA, from time to time (the "Supporting Documentation").

d) The Requestor or their authorized representative must be requesting the Information only in order to try and resolve the Dispute, and the Information, if provided, may not be used (in whole or in part) for any other reason.

e) The Requestor or their authorized representative must have both: (a) attempted to send a message regarding the Dispute to the Registrant through the Interested Party Contact Procedure (accessible on the CIRA website), no less than 14 calendar days prior to this request; and (b) was not able to resolve the Dispute through this mechanism. Communications through other means, or regarding other matters, do not satisfy this requirement.

f) The request for the Information of the Registrant must be in the applicable form as specified by CIRA from time to time. The form must be: (i) accurately and fully completed; (ii) signed by the Requestor or their appointed representative, certifying full compliance with the requirements of these Rules and Procedures and that the information in the form is truthful and correct; and (iii) the original sent by postal mail, courier or delivered in person to the address specified in the form.

g) The form must be accompanied by the applicable Supporting Documentation.

4. CIRA Response. CIRA will respond to the request as quickly as possible after receipt of a form. CIRA reserves the right not to respond to a request, or to refuse a request where the Requestor did not, or CIRA believes may not, fully comply with all of the requirements of these Rules and Procedures.

5. Notice to Registrant. If CIRA approves a request hereunder, CIRA shall, unless prohibited by law, not less than 30 and not more than 60 days after disclosure of the Information, use reasonable efforts to send an email to the Administrative Contact of the Registrant indicating: (a) that CIRA has disclosed the Information; and (b) the name of the Requestor to whom CIRA has disclosed the Information.

REQUEST FOR DISCLOSURE OF REGISTRANT INFORMATION

1. Contact information for person making the request ("Requestor"):

Name: _____

Postal Address: _____

_____

_____

Email Address: _____

2. If this request is made on behalf of another person, the contact information for that person:

Name: _____

Postal Address: _____

_____

_____

Email Address: _____

3. Specify the CIRA domain name for which the Information is being requested (Note: If Information is being requested regarding more than one domain, a separate Request Form is required for each domain):

_____

4. Check mark the type of Dispute for which you are making this request, and attach the required Supporting Documentation:

	Dispute	**Required Supporting Documentation**
☐	Registered Canadian Trade-mark	Certified or Notarized copy of Canadian Trademark Registration
☐	Registered Canadian Copyright	Certified or Notarized copy of Canadian Copyright Registration
☐	Registered Federal or Provincial corporate, business or trade name	Federal or Provincial Corporations: Current Certificate of Status or equivalent document, e.g. Certificate of Compliance, Certificate of Good Standing Certified Business or Trade Names: Certified Detailed Business Name Report
☐	Issued patent	Certified or Notarized copy of Canadian Patent
☐	Identity Theft	1. Completed Identity Theft Statement, available from the Consumer Measures Committee : Available at http://www.cmcweb.ca/epic/site/cmc-cmc.nsf/vwapj/IDTheftStatement.pdf/$FILE/IDTheftStatement.pdf and

2. Proof of identity (Notarized Copy of a valid document issued by a federal, provincial, municipal authority, which must include the bearer's name and signature. For example: Provincial driver's licence, Provincial health care card, Other provincial identification card, Other federal identification card, Certificate of Indian Status, Old Age Security card, Federal, provincial or municipal employee identification card, or Canadian passport).

5. Indicate the specific date in which you sent correspondence to the Registrant through the Interested Party Contact Procedure, regarding the Dispute (dd/mm/yy):_____

6. I certify that I have fully complied with the requirements of these Rules and Procedures, including without limitation:

a) I, or the person I am authorized to represent, have a current, good faith Dispute with a Registrant, as indicated above;

b) I have attempted to communicate with the Registrant regarding the Dispute through the Interested Party Contact Procedure, no less than 14 calendar days prior to this request, but have not been able to resolve the Dispute through this mechanism;

c) This request is made in good faith for the purposes of attempting to resolve the Dispute with the Registrant, and I will use the Information received through this request solely for the purposes of resolving the Dispute with the Registrant, and for no other purpose; and

d) All the information set out in this request form is complete and correct.

Signature: _____

Name: _____

Title or capacity (if applicable): _____

Date: _____

Please submit one original signed copy of the completed form in person, by postal mail or courier to:

Disclosure Requests
Canadian Internet Registration Authority
979 Bank Street
Suite 400
Ottawa, Ontario
K1S 5K5

APPENDIX H

Manila Principles on Intermediary Liability

Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation

A GLOBAL CIVIL SOCIETY INITIATIVE

Version 1.0, March 24, 2015

Manila Principles on Intermediary Liability

Introduction

All communication over the Internet is facilitated by intermediaries such as Internet access providers, social networks, and search engines. The policies governing the legal liability of intermediaries for the content of these communications have an impact on users' rights, including freedom of expression, freedom of association and the right to privacy.

With the aim of protecting freedom of expression and creating an enabling environment for innovation, which balances the needs of governments and other stakeholders, civil society groups from around the world have come together to propose this framework of baseline safeguards and best practices. These are based on international human rights instruments and other international legal frameworks.

Uninformed intermediary liability policies, blunt and heavy-handed regulatory measures, and a lack of consistency across these policies has resulted in censorship and other human rights abuses by governments and private parties, limiting individuals' rights to free expression and creating an environment of uncertainty that also impedes innovation online.

The framework presented here should be considered by policymakers and intermediaries when developing, adopting, and reviewing legislation, policies and practices that govern the liability of intermediaries for third-party content. Our objective is to encourage the development of interoperable and harmonized liability regimes that can promote innovation while respecting users' rights in line with the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the United Nations Guiding Principles on Business and Human Rights.

I. Intermediaries should be shielded from liability for third-party content

a) Any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible.

b) Intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.

c) Intermediaries must not be held liable for failing to restrict lawful content.

d) Intermediaries must never be made strictly liable for hosting unlawful third-party content, nor should they ever be required to monitor content proactively as part of an intermediary liability regime.

II. Content must not be required to be restricted without an order by a judicial authority

a) Intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful.

b) Orders for the restriction of content must

   1. Provide a determination that the content is unlawful in the jurisdiction.

   2. Indicate the Internet identifier and description of the unlawful content.

   3. Provide evidence sufficient to document the legal basis of the order.

   4. Where applicable, indicate the time period for which the content should be restricted.

c) Any liability imposed on an intermediary must be proportionate and directly correlated to the intermediary's wrongful behavior in failing to appropriately comply with the content restriction order.

d) Intermediaries must not be liable for non-compliance with any order that does not comply with this principle.

III. Requests for restrictions of content must be clear, be unambiguous, and follow due process

Consistent with Principle II, intermediaries should not be required to restrict content without an order from a judicial authority. In the event that governments or private complainants request content restriction, the following principles apply.

a) Intermediaries must not be required to substantively evaluate the legality of third-party content.

b) A content restriction request pertaining to unlawful content must, at a minimum, contain the following:

    1. The legal basis for the assertion that the content is unlawful.

    2. The Internet identifier and description of the allegedly unlawful content.

    3. The consideration provided to limitations, exceptions, and defences available to the user content provider.

    4. Contact details of the issuing party or their agent, unless this is prohibited by law.

    5. Evidence sufficient to document legal standing to issue the request.

    6. A declaration of good faith that the information provided is accurate.

c) Content restriction requests pertaining to an intermediary's content restriction policies must, at the minimum, contain the following:

    1. The reasons why the content at issue is in breach of the intermediary's content restriction policies.

    2. The Internet identifier and description of the alleged violation of the content restriction policies.

    3. Contact details of the issuing party or their agent, unless this is prohibited by law.

    4. A declaration of good faith that the information provided is accurate.

d) Intermediaries who host content may be required by law to respond to content restriction requests pertaining to unlawful content by either forwarding lawful and compliant requests to the user content provider, or by notifying the complainant of the reason it is not possible to do so ('notice and notice'). Intermediaries should not be required to ensure they have the capacity to identify users.

e) When forwarding the request, the intermediary must provide a clear and accessible explanation of the user content provider's rights, including in all cases where the intermediary is compelled by law to restrict the content a description of any available counter-notice or appeal mechanisms.

f) If intermediaries restrict content hosted by them on the basis of a content restriction request, they must comply with Principle VI on transparency and accountability below.

g) Abusive or bad faith content restriction requests should be penalized.

IV. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality

Laws, orders and practices restricting content must be necessary and proportionate in a democratic society:

a) Any restriction of content should be limited to the specific content at issue.

b) When restricting content, the least restrictive technical means must be adopted.

c) If content is restricted because it is unlawful in a particular geographical region, and if the intermediary offers a geographically variegated service, then the geographical scope of the content restriction must be so limited.

d) If content is restricted owing to its unlawfulness for a limited duration, the restriction must not last beyond this duration, and the restriction order must be reviewed periodically to ensure it remains valid.

V. Laws and content restriction policies and practices must respect due process

a) Before any content is restricted on the basis of an order or a request, the intermediary and the user content provider must be provided an effective right to be heard except in exceptional circumstances, in which case a *post facto* review of the order and its implementation must take place as soon as practicable.

b) Any law regulating intermediaries must provide both user content providers and intermediaries the right of appeal against content restriction orders.

c) Intermediaries should provide user content providers with mechanisms to review decisions to restrict content in violation of the intermediary's content restriction policies.

d) In case a user content provider wins an appeal under (b) or review under (c) against the restriction of content, intermediaries should reinstate the content.

e) An intermediary should not disclose personally identifiable information about a user without an order by a judicial authority. An intermediary liability regime must not require an intermediary to disclose any personally identifiable user information without an order by a judicial authority.

f) When drafting and enforcing their content restriction policies, intermediaries should respect human rights. Likewise, governments have an obligation to ensure that intermediaries' content restriction policies respect human rights.

VI. Transparency and accountability must be built into laws and content restriction policies and practices.

a) Governments must publish all legislation, policy, decisions and other forms of regulation relevant to intermediary liability online in a timely fashion and in accessible formats.

b) Governments must not use extra-judicial measures to restrict content. This includes collateral pressures to force changes in terms of service, to promote or enforce so-called "voluntary" practices and to secure agreements in restraint of trade or in restraint of public dissemination of content.

c) Intermediaries should publish their content restriction policies online, in clear language and accessible formats, and keep them updated as they evolve, and notify users of changes when applicable.

d) Governments must publish transparency reports that provide specific information about all content orders and requests issued by them to intermediaries.

e) Intermediaries should publish transparency reports that provide specific information about all content restrictions taken by the intermediary, including actions taken on government requests, court orders, private complainant requests, and enforcement of content restriction policies.

f) Where content has been restricted on a product or service of the intermediary that allows it to display a notice when an attempt to access that content is made, the intermediary must display a clear notice that explains what content has been restricted and the reason for doing so.

g) Governments, intermediaries and civil society should work together to develop and maintain independent, transparent, and impartial oversight mechanisms to ensure the accountability of the content restriction policies and practices.

h) Intermediary liability frameworks and legislation should require regular, systematic review of rules and guidelines to ensure that they are up to date, effective, and not overly burdensome. Such periodic review should incorporate mechanisms for collection of evidence about their implementation and impact, and also make provision for an independent review of their costs, demonstrable benefits and impact on human rights.