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