March 16, 2018

RE: Technical Comment on FairPlay Canada's proposal to CRTC on Disabling Access to Piracy Sites

1. The Internet Society is pleased to submit the following comment on the potential negative impacts of disabling access to piracy sites in the FairPlay Canada's proposal to the Canadian Radio-Television and Telecommunications Commission (CRTC) titled Application Pursuant To Sections 24, 24.1, 36 And 70(1)(A) of the Telecommunications Act, 1993 to Disable On-Line Access to Piracy Sites.

2. The Internet Society is a global not-for-profit organization committed to making the Internet available to everyone, everywhere. Working in partnership with our global community, comprised of more than 100,000 individual members, 130 chapters and special interest groups across the world (including two chapters in Canada) and 149 organizational members, the Internet Society provides leadership and expertise on policy, technology and communications matters. The Internet Society is also the organizational home of the Internet Engineering Task Force and the Online Trust Alliance.[1]

3. 'Disabling access' is a generic description for a process where an Internet Service Provider (ISP) may open and examine a user's data packets or data headers to determine if the user is requesting a Domain Name Service (DNS) resolution for a site that has been deemed to be inappropriate or illegal in a particular jurisdiction. If so, the ISP blocks, redirects or otherwise disables such a request for resolution of the domain name. This process is properly referred to as DNS filtering or blocking. The user is then unable to obtain a numerical address for the deemed piracy site and therefore cannot communicate with the given site.

4. "Disabling Access" to piracy sites is only briefly mentioned in FairPlay coalition's proposal as something to be undertaken by ISPs, as directed by an independent body, the "Independent Piracy Review Agency" (IPRA), who determine which sites are involved in piracy and should be blocked. However, we believe it is critical to understand how the coalition plans to block access to websites deemed offensive.

5. It is disconcerting that while the FairPlay coalition's proposal outlines what the coalition believes needs to be done, the proposal is short on crucial details as to how the coalition will actually carry out those actions. Of particular concern to the Internet Society is the process ISPs will use to block Canadians' access to sites deemed offensive. This is not a detail to be

[1] https://www.internetsociety.org/

internetsociety.org
@internetsociety
Galerie Jean-Malbuisson 15,
Geneva, CH-1204 Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
1775 Wiehle Ave, Suite 201,
Reston, VA 20190 USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

worked out at a later date; it is crucial to understand upfront as history has shown that the preferred method for doing so – blocking, redirecting or disabling access to websites – can negatively impact the security and stability of the Internet, infringe on the privacy of end users, can curtail legitimate speech, and may inadvertently block legitimate websites in their entirety.

6. In many countries and regions where attempts have been made to block piracy sites, blocking online content has resulted in a storm of protests from experts and the general public as it can fundamentally break the Internet as we know it today.[2] In the long run, it has also proven to be an expensive[3] and ineffective[4] course of action. Therefore, the Internet Society wishes to ensure the CRTC has a thorough understanding of the effects (and side effects) in its consideration of the FairPlay proposal.

7. To this end, we respectfully submit the attached brief, *Perspectives on Content Blocking: An Overview,* published by the Internet Society in March 2015. In this brief, we outline the various techniques employed to block content online, and evaluate each technique in terms of both its effectiveness and potential negative impacts on the Internet, Internet security and end user privacy. Our assessment identifies two main drawbacks common to all blocking techniques:

> "They do not solve the problem. Blocking techniques do not remove content from the Internet, nor do they stop the illegal activity or prosecute culprits; they simply put a curtain in front of the content. The underlying content remains in place.
>
> They inflict collateral damage. Every blocking technique suffers from over-blocking and under-blocking: blocking more than is intended and, at the same time, less than intended. They also cause other damage to the Internet by putting users at risk (as they attempt to evade blocks), reducing transparency and trust in the Internet, driving services underground, and intruding on user privacy. These are costs that must be considered at the same time that blocking is discussed."[5]

---

[2] See *Quebec to require ISPs to block websites:* http://internetsociety.ong/blog/north-america-bureau/2016/07/quebec-require-isps-block-websites (Internet Society); *The Domain Name System: Finding Solutions to Illegal On-line Activities:* http://www.isoc.org/internet/issues/dns-filtering.shtml (Internet Society); Letter from Steve Crocker, PhD, David Dagon, PhD, Dan Kaminsky, Danny Mcpherson, and Paul Vixie, PhD regarding *S.968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act and H.R.3261, Stop Online Piracy Act:* http://www.circleid.com/pdf/letter-to-us-hr-regarding-sopa.pdf; *The Stop Online Piracy Act (SOPA):* https://cira.ca/blogs/public-domain/stop-online-piracy-act-sopa (CIRA); *Regarding CRTC's opinion that Quebec cannot block access to gambling sites:* https://cira.ca/blog/state-internet/regarding-crtc%E2%80%99s-opinion-quebec-cannot-block-access-gambling-sites (CIRA).

[3] *Three Strikes Anti-Piracy Budget "Too Expensive To Justify" Says Minister:* https://torrentfreak.com/three-strikes-anti-piracy-budget-too-expensive-to-justify-says-minister-120603/ (TorrentFreak).

[4] *Perspectives on Domain Name System (DNS) Filtering:* http://www.isoc.org/internet/issues/dns-filtering.shtml (Internet Society).

[5] *Perspectives on Content Blocking: An Overview:* https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/ (Internet Society).

8. More specifically, DNS is one of the fundamental protocols on which overall global Internet functionality is built. DNS filtering causes instability, encourages fragmentation, and erodes the foundation of the Internet. Domain name seizure suffers from most of the same problems as DNS filtering, including easy circumvention, failure to solve the underlying problem, and encouragement of a shadow network out of reach of law enforcement.

- Unilateral modification of DNS behavior carries high security risks. DNS filtering is incompatible with DNSSEC[6] and encourages the creation of alternative, non-standard DNS systems. These alternative systems reduce global Internet security and put individual users at risk. Because almost every system and service in the Internet depends on DNS, filtering will affect more users than are intended. What is filtered in Pakistan may affect users in Panama. Filtering creates a highly fragmented, country-by-country Internet rather than one global network. *Filtering the global DNS has risks to users and will decrease global security.*
- Filtering DNS does not solve the problem. Changing the DNS doesn't remove the objectionable or illegal content from the Internet; it makes it simply harder to get to. Users who are determined to download this type of material will still be able to do so. If DNS filtering is used in many countries, then users will also set up "shadow" Internet structures to avoid filtering, making it more difficult for law enforcement to observe and intervene. *Policy makers should focus on the most effective ways to solve the problem.*
- Filtering DNS causes significant collateral damage. We have abundant anecdotal evidence that DNS filtering will affect users and content providers engaging in completely legal activities. For example, in February 2011, U.S. authorities blocked the domain "mooo.com," because some child pornography was found on a sub-domain. The blockage also affected over 80,000 other legal web sites set up as sub-domains of mooo.com. In some cases, collateral damage can be minimized by very careful technical implementation, but it can never be eliminated. *The cost of DNS filtering outweighs possible short-term benefits.*
- DNS filtering has non-technical implications. The fundamental issue is non- technical: how to keep illegal content off of the Internet. Solving this non-technical problem with technology, such as DNS filtering, raises privacy and public policy issues. DNS filtering erodes trust in the Internet when users are no longer certain that typing www.isoc.org into a web browser will get them to the ISOC web site. To address the issues of illegal online activities, policy makers need to act in accordance with basic international norms including the rule of law and standards of due process. *"Quick and easy" technical solutions to non-technical problems must be considered carefully to avoid infringing internationally-agreed human rights and eroding trust in the Internet.*
- The real solution to combating illegal activities is to attack them at the source, through international cooperation. These are cross-border issues and cannot be effectively

[6] To thwart DNS spoofing or man-in-the-middle attacks, the Internet Engineering Task Force has developed a technology called DNSSEC (DNS SECurity) that uses digital signatures to authenticate the origin of a DNS data. But if DNS filtering is mandated, it will thwart the deployment of DNSSEC as a way of securing the Internet. In effect the ISP is "poisoning" the DNS entry in the same way a criminal would do with DNS spoofing and thereby breaking the trust model that powers the Internet DNS system.

solved on a country-by-country basis. A continuing dialogue between national authorities and the Internet community can help. For example, better authentication of DNS name registrants would allow for the possibility of tracking back bad behavior to an identifiable person, which itself may act as a deterrent. Other levers, such as attacking the payment systems used by cyber-criminals, may also yield longer-lasting and more effective results. *International cooperation provides the appropriate avenue for policymakers and the technical community to solve this problem.*

8. "Disabling Access" to piracy sites may seem like an innocuous term but it glosses over serious implications on how this technology can undermine the basic functionality of the Internet. The decision to move forward, or not to move forward, with the FairPlay Coalition's proposal should only be taken after a full examination of the potentially negative effects of on the security and stability of the Internet, the privacy of Canadians, and how it may inadvertently block legitimate websites. In our opinion, the negative impacts of disabling access greatly outweigh any benefits. The Internet Society encourages the CRTC to review the attached brief and consider alternative approaches to minimize the impact of pirated content online.