

Fact checking Michael Geist's criticisms of the FairPlay site blocking proposal

by Barry Sookman

March 28, 2018

available at

<http://www.barrysookman.com>

Table of Contents

Part 1: Summary and FAQ	5
Is the proposal “radical”; is site blocking is quite rare?	5
Would Canada be a “virtual outlier” and is the proposal “fatally flawed” because the CRTC and not courts will make the blocking orders?	5
Do human rights norms require courts to make blocking orders?	6
Would the proposal violate net neutrality rules?	6
Is website blocking effective?	7
Would the proposal inevitably lead to widespread over-blocking of legal content?	7
Would the proposal violate freedom of expression rights?	8
Would the proposal increase privacy risks for Canadians?	9
Would the proposal inevitably result in blocking for other purposes?	9
Does Canada have robust laws so that more legal tools to target offshore pirate sites?	10
Why this matters?	11
Part 2: Detailed review and analysis of Geist’s claims	12
Geist claim: site blocking is quite rare; the proposal is “radical”	12
Geist claim: Other countries don’t empowers government agencies to make blocking orders	15
Geist claim: blocking orders must be made by courts	18
Geist claim: Human rights norms require courts to make blocking orders	23
Geist claim: the proposal will violate Canadian net neutrality rules	28
Geist claim: website blocking is not effective	36
Geist claim: The proposal will lead to widespread over-blocking of legal content.....	52
Geist claim: website blocking may violate human rights	56
Geist claim: the proposal will lead to higher Internet access costs for all	68
Geist claim: the proposal would increase privacy risks	72
Geist claim: slippery slope; it will inevitably result in blocking for other IP purposes.....	77

Geist claim: more slippery slopes; the proposal will lead to blocking for other purposes.....	78
Geist claim: more slippery slopes, the proposal will turn the CRTC into a content regulatory authority	84
Geist claim: Canada has robust laws and doesn't need more legal tools to target offshore pirate sites.....	85
Why all this matters - Conclusion.....	89

Fact checking Michael Geist's criticisms of the FairPlay site blocking proposal – by Barry Sookman

March 28, 2018 available at barrysookman.com

The FairPlay coalition comprising more than 25 organizations representing hundreds of thousands of members of Canada's creative community made a reasonable proposal to the Canadian Radio-television and Telecommunications Commission (CRTC), Canada's telecommunications and broadcast regulator, to address the scourge of online copyright infringement.¹ The proposal, which involves website blocking, was immediately attacked by anti-copyright activist Michael Geist ("Geist") in a series of articles and interviews. As I showed in a [prior lengthy blog post](#),² his criticisms were unfounded and overblown.

Geist has renewed his attack on the proposal in new series of articles that expand upon his previous and other themes.³ His criticisms do not withstand scrutiny. They are based on inaccurate and misleading facts and arguments, unsubstantiated and incorrect assertions about international norms and Canadian and international law. He makes selective and misleading use of references and quotations and relies on cases that have been overturned or superseded by subsequent courts.

This article examines his claims and the references he uses to support them. I start with a short summary and FAQ and then provide a detailed comprehensive review and analysis of his claims.

¹ The research assistance of Simon Cameron is gratefully acknowledged.

² Barry Sookman "[Why the CRTC should endorse FairPlay's website-blocking plan: a reply to Michael Geist](http://www.barrysookman.com/2018/02/12/why-the-crtc-should-endorse-fairplays-website-blocking-plan-a-reply-to-michael-geist/)", Feb 12, 2018, <http://www.barrysookman.com/2018/02/12/why-the-crtc-should-endorse-fairplays-website-blocking-plan-a-reply-to-michael-geist/>. (*Sookman Why the CRTC should endorse FairPlay's website-blocking plan*).

³ Geist's blog post's are listed and summarized in his post "The Case Against the Bell Coalition's Website Blocking Plan, The Finale", March 8, 2018, <http://www.michaelgeist.ca/2018/03/caseagainstsiteblockingfinale/>. Also, his posts "Outlier: Why Bell's Leadership on Website Blocking Places It at Odds With Telecom Companies Around the World" and "Outlier, Part 2: What is the CBC Doing Supporting Website Blocking?" on his website michaelgeist.ca.

Part 1: Summary and FAQ

Is the proposal “radical”; is site blocking is quite rare?

Geist says the proposal is radical and that site blocking is rare. He is wrong.

Website blocking is hardly rare. It is one of the leading anti-piracy mechanisms of recent years.

It is also hardly “radical”. It is available in at many countries including liberal democratic countries such as Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Norway Portugal, Sweden, Spain, UK, Mexico, Australia, and Singapore.

Further, courts and government agencies from around the world have rejected the arguments that Geist makes against the proposal. The numerous decisions and the practices around the world show that his claims that website blocking for copyright purposes will result in over-blocking, will not be effective, may violate human rights or net neutrality principles, and that orders must be made by courts and not government agencies, are not correct.

Would Canada be a “virtual outlier” and is the proposal “fatally flawed” because the CRTC and not courts will make the blocking orders?

Not at all; the information provided by Geist is inaccurate.

Geist’s claim that there is effectively only one country that allows administrative agencies to permit website blocking for copyright purposes is wrong. There are at least 7 countries which empower government agencies to make orders requiring website blocking for copyright purposes.

Moreover, the CRTC has all of the powers it requires to ensure a fair hearing for sites that may be blocked and its decisions are subject to ample judicial oversight.

The CRTC has the relevant powers of a court of superior jurisdiction and already makes decisions that affect the fundamental freedoms of Canadians. This includes when regulating Canada’s communication system and enforcing the Unsolicited Telecommunications Rules, CASL, the National Do Not Call List (DNCL) and the VCR.

Canadian courts have repeatedly concluded that administrative bodies such as the CRTC may issue orders requiring a consideration of human rights or *Charter* values. Administrative bodies in Canada can, and do, make decisions with important consequences that affect human rights.

Do human rights norms require courts to make blocking orders?

They do not. Geist is “selective” in the sources he relies on to make this claim.

His claim is contradicted by a report to the United Nations on freedom and expression on the Internet that he and the Electronic Frontier Foundation previously lauded and that recognized that blocking orders can be made by courts or an independent body.

Geist’s claim is contradicted by the Guideline published by the Council of Europe related to the use of blocking to protect freedom of expression in the EU under the *European Convention on Human Rights*.

His claim is contradicted by international norms as many countries including Italy, Mexico, South Korea, France, and others permit blocking orders to be made by government agencies for copyright or other purposes.

Would the proposal violate net neutrality rules?

It would not and Geist provides no credible argument that this would be the case.

Geist says that “net neutrality is the right for users to access content and applications of their choice, blocking content is prima facie a net neutrality violation.”

It is not. He is also wrong when he says the “no blocking” principle prevents courts or other lawful authorities from taking measures to protect the public from online illegal threats and menaces. If such a rule existed, it would be both surprising and dangerous. It would create the incongruity that what is unlawful and can be enjoined offline cannot be enjoined online. Such a radical view of net neutrality would undermine the rule of law on the Internet and accountability and responsibility in Internet Governance.

Canada’s major trading partners including the United States and the European Union recognize that net neutrality rules do not prevent courts or government agencies from ordering the removal of illegal content from the Internet.

In the U.S. the net neutrality rules expressly exclude illegal materials. In the EU, the rules expressly permit orders of courts and public bodies to make blocking orders. In fact, Italy, Greece, Portugal and Poland use government agencies to make such orders.

Canada's *Telecommunications Act*, as interpreted by the CRTC, gives the CRTC the express authority to approve blocking orders. It is wrong to claim that if the CRTC makes an order requiring ISPs block foreign piracy sites that such an order would violate Canada's net neutrality law.

Geist's view of net neutrality is not consistent with the Canadian government's understanding of Canada's net neutrality framework as well. Referring to the proposal, Minister Bains confirmed the "Government supports an open Internet where Canadians have the ability to access the content of their choice in accordance to Canadian laws... In other words, our Government believes that all legal content must be treated equally by internet service providers."

The CRTC has said in past decisions it would make blocking orders if making the order would be consistent with the objectives of the *Telecommunications Act*. This is precisely what the coalition is asking the Commission to do.

Is website blocking effective?

Yes; many studies and court decisions have found this to be the case.

Geist is again "selective" in the reports he cites and on the parts of the reports he refers to when he argues web site blocking is not effective. Studies in the UK (several), Australia (2), South Korea, and Portugal have all found website blocking to be an effective means of reducing piracy.

Geist failed to refer to the leading academic study on site blocking (Prof. Danaher 2016) which found site blocking to be effective in reducing visits to the blocked piracy sites, to other piracy sites not blocked, and in increasing visits to legal sites.

Geist also ignores the plethora of decisions throughout the EU and elsewhere that made express findings that site blocking is an effective remedy against online copyright piracy. Instead he relies on a single decision of a Danish court that was reversed on appeal precisely on this point.

Would the proposal inevitably lead to widespread over-blocking of legal content?

Geist presents no credible reason why this would occur and cases in other countries have concluded that site blocking can be safely carried out without over-blocking.

Geist merely lists instances of reported over-blocking in random cases and concludes it will necessarily occur when blocking orders are made by the CRTC. He gives no explanation as to why over-blocking cannot be avoided. In fact, the potential causes are well known and can be addressed.

Moreover, while purporting to be concerned about over-blocking, Geist completely neglects and appears to be unconcerned about under-blocking—that is, the ready access to infringing materials made available on a mass scale by those who have built business models profiting from it. He advances a test of the status quo – everything is fine with no over-blocking – with rampant unchecked piracy over the inadvertent, occasional, avoidable, and reversible potential cases of over-blocking.

Geist also ignores the numerous international decisions that have rejected claims that such orders result in over-blocking and where decision makers take steps to mitigate such risks. These courts and government agencies are as concerned as the CRTC would be to avoid over-blocking and to prevent the damaging consequences of under-blocking.

Would the proposal violate freedom of expression rights?

It would not. There is substantial jurisprudence in Europe and elsewhere that find blocking orders to be fully compatible with human rights including freedom of expression rights.

The proposal targets only sites that blatantly, overwhelmingly, or structurally engage in piracy. Legitimate websites are not targeted by the proposal.

All members of the coalition depend on Canada maintaining strong laws that protect freedom of expression on the Internet. But, contrary to Geist's implications, freedom of expression is not absolute either on or off the Internet. It does not extend to permit pirate sites or their users to shield illegal actions under a banner of freedom of expression.

Countries around the world with strong freedom of expression rights guarantees have made blocking orders for copyright purposes.

Geist claims to have reviewed “many of the site blocking cases from around the world”. Yet he completely ignores the significant body of caselaw from around the world that has found website blocking orders to be proportionate and not to violate fundamental values including constitutionally protected rights of freedom of expression.

He ignored a contrary decision from the Court of Justice of the European Union and from courts in Argentina, Belgium, Finland, France, Germany, Ireland, Netherlands, Norway, and the UK, among others. He preferred instead to rely on an outdated secondary source that references decisions in Germany and the Netherlands that were reversed or superseded by later developments and several blocking orders issued in each of Germany and the Netherlands. These authorities found blocking orders to be consistent with fundamental human rights.

Would the proposal increase privacy risks for Canadians?

It would not. If anything, It would lessen any privacy risks.

Geist gives several reasons for his assertion that the proposal would increase privacy risks for Canadians. None of them stand up to scrutiny.

He says it will lead to blocking VPNs used to illegally access U.S. Netflix. There is no reason to assume this will happen or to attribute that to the proposal.

He says personal information will be collected for rights holders to get and implement blocking orders. This ignores the fact that one of the benefits of blocking orders is that they are directly targeted at the pirate sites and not individual users. The information needed to obtain a blocking order is publicly available on the pirate site and through Alexa data and does not need to include any subscriber personal information.

In addition, the proposal does not raise any incremental privacy issues that would not arise in legal proceedings against piracy sites.

Geist also fails to consider that the type of pirate websites targeted are known for harvesting and misusing personal information and hijacking users' computers.

Would the proposal inevitably result in blocking for other purposes?

Geist offers no evidence in support of this claim and he ignores the fact that the proposal calls for blocking of only "websites and services that are blatantly, overwhelmingly, or structurally engaged in piracy." The proposal does not seek the CRTC's authority to block web sites for any other purpose.

If the CRTC or Parliament later chose to adopt a separate, highly targeted blocking regime to deal with sites that are clearly devoted to dissemination of illegal content (as has existed for

years for child pornography), that would not be a reason to oppose the FairPlay proposal. Other liberal democratic countries already engage in website blocking to protect members of the public from a variety of illegal activities such as hate speech, child abuse materials including child pornography, prostitution, speech inciting violence, and terrorism.

Geist also tries to conflate blocking illegal pirate sites to content regulation. That is no more true than arguing that when courts grant injunctions prohibiting the dissemination of materials that are defamatory, in violation of child pornography or pornography laws, infringe copyrights, or are otherwise illegal - which courts do all the time – they are engaging in “content regulation”.

We need to recognize that what is illegal offline is illegal online. Effective remedies need to be available in both situations to protect the public.

Does Canada have robust laws so that more legal tools to target offshore pirate sites?

Website blocking is the most effective means of dealing with online piracy from foreign sites. Other laws would either be completely ineffective or much less effective than site blocking.

Geist claims Canada “has some of the world’s toughest anti-piracy provisions” and doesn’t need any new laws to target online piracy.

Although Geist makes references to anti-piracy laws that exist in Canada, he makes no attempt to show whether or how they could be useful in combatting the threats the FairPlay proposal is designed to counter. Many of his claims would be misleading to the average person who would not understand the lack of connection between an existing cause of action and one that had some relevance to countering online piracy.

It is not true that merely because Canada has some laws that are in line with those of our major trading partners, such as measures to counter trafficking in anti-circumvention devices, a contributory infringement (enablement) cause of action, and measures that may be able to target individuals selling fully loaded Kodi boxes or other ISDs, that these same laws would be effective against foreign online pirate sites.

Direct enforceable remedies against operators of pirate sites is frequently impossible. The Pirate Bay has been blocked around the world and its originators were jailed by a Swedish court. Yet, it still continues to defy and evade legal measures to shut it down.

Geist also misleadingly points to the possibility of high damages awards against the operators of piracy sites, neglecting the fact that the availability of such awards is meaningless unless the award can be enforced.

Genuine efforts to stem online piracy require a mixture of complementary and appropriate measures including web site blocking. That is why throughout the European Union and in other countries around the world orders against ISPs are used to block the sources of illegal content that facilitate infringements on a mass scale.

Why this matters?

The FairPlay proposal represents a well thought out approach to dealing with Internet piracy in the Canadian context. Yet, Geist has attempted to demonize it using, what appears to be, every contrived argument he can think of.

Geist postulates a radical net neutrality Internet Governance framework where courts and government agencies are powerless to intervene to halt illegal activities over the Internet. He takes a similarly unbalanced position in claiming that intervening to stop online theft is unnecessary by ignoring or discounting the well documented harms caused by illegal piracy sites, the evidence that blocking orders are effective without any real risks of over-blocking and do not breach fundamental freedom of speech rights or net neutrality principles.

What is especially troubling is that he tells average Canadians – people who would have no reason to disbelieve a Canada Research Chair - that the proposal is radical, breaks net neutrality rules, may violate their fundamental freedom of speech and privacy rights, will result in blocking access to U.S. Netflix, content blocking by the CRTC, and will lead to who knows what else. This is fearmongering, plain and simple.

Unfortunately, but quite predictably, his unfounded attacks are being relied upon by others including OpenMedia to oppose the proposal using exaggerated and inflammatory arguments. The result of all of this is that a large number of the submissions to the CRTC have been influenced directly or indirectly by Geist's misleading diatribes against the proposal.

We, as Canadians, have an important interest in ensuring that debates on important issues do not get subverted by misinformation. I therefore encourage those who want to have a more complete understanding of the issues to read this article in full.

The FairPlay proposal should be assessed on its merits based on a careful analysis of the facts and evidence. We should not allow widely circulated misinformation be a factor governing decisions about important matters of public policy including the proposal.

What follows is a detailed analysis of Geist's criticisms of the proposal in his recent series of blog posts.⁴

Part 2: Detailed review and analysis of Geist's claims

Geist claim: site blocking is quite rare; the proposal is "radical"

Geist claims that "website blocking for copyright purposes is still quite rare". He also calls the proposal "radical". Neither claim is accurate.

The term "rare" means "not occurring or found very often". The term "quite" means "to the greatest degree".⁵ You might infer this means almost never. His claim is not accurate by any sense of the terms. According to TorrentFreak, an online publication dealing with illegal filesharing and anti-piracy litigation:

Website blocking has become one of the leading anti-piracy mechanisms of recent years.

It is particularly prevalent across Europe, where thousands of sites are blocked by ISPs following court orders.⁶

Blocking pirate sites is also not "radical". Site blocking (or other online location blocking) for copyright purposes is widely available in liberal democratic countries. It is available, for example, in EU/EEA member states (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Norway, Portugal, Sweden, Spain, UK, and the legal basis also

⁴ This article doesn't deal with arguments I have already dealt with extensively in my prior blog post since Geist make no new substantive arguments, namely, "Part 2: Weak Evidence on the State of Canadian Piracy" and "Part 3: Piracy Having Little Impact on Thriving Digital Services and TV Production". The article also doesn't deal expressly with "Part 13: It is Inconsistent With the CRTC Policy Direction", "Part 14: Failure To Further the Telecommunications Act Policy Objectives", "Part 15: It Undermines the Telecommunications Act Policy Objectives", as these issues are largely repetitions of his prior arguments under new headings and because these are extensively addressed in the opinion filed along with the proposal which Geist does not attempt to counter.

⁵ Pocket Oxford English Dictionary 9th ed. (Oxford University Press) 2001

⁶ Ernesto, "Pirate Site Blockades Enter Germany With Kinox.to as First Target", Feb 13, 2018, <https://torrentfreak.com/pirate-site-blockades-enter-germany-with-kinox-to-as-first-target-180213/>; also, Ernesto, "Blocking Pirate Sites Without a Trial is Allowed, Italian Court Rules" Torrentfreak, Apr. 3, 2017 available at <https://torrentfreak.com/blocking-pirate-sites-without-a-trial-is-allowed-italian-court-rules-170403/>.

exists in the other member states of the European Union based on Article 8(3) of the *Infosoc Directive*),⁷ South America/Latin America (Mexico, Argentina), and Eurasia and Australasia (Australia, India, Indonesia, Malaysia, Russia, Turkey, Singapore, South Korea, Thailand).⁸ Secondary sources also suggest it may be available in Brazil, Chile, Peru, and Saudi Arabia.⁹ In some cases countries have specific laws that establish a regime for the blocking. In other cases it is available under generally applicable civil law, constitutional law, or administrative law rules.¹⁰ Japan is also considering site blocking to protect Manga and anime, important content in Japan.¹¹

Further, as summarized below, courts and government agencies from around the world have canvassed the issues raised by Geist and have found it appropriate to make, and have made, blocking orders. Examples of such cases in the English language include those from United Kingdom¹², Ireland,¹³ Australia,¹⁴ and from the Court of Justice of the European Union.¹⁵ There

⁷ “Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society”, Official Journal L 167 , 22/06/2001 P. 0010 – 0019, 22 May 2001, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>, “Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.”

⁸ Jo Oliver and Elena Blobel, “Website Blocking injunctions – A Decade of Development”, in Jacques de Werra (Ed) et al, *Droit d’auteur 4.0*, Schulthess Verlag (2018) (“*Oliver Website Blocking injunctions*”) at 32-42, 52-53. According to this article, website blocking in Mexico is limited to operators of targeted websites that have a physical address in Mexico. The same may be true in Brazil. See, also, Cory, Nigel, ITIF, *How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet”*, August 2016, <http://www2.itif.org/2016-website-blocking.pdf> at p. 13,

⁹ *Oliver Website Blocking injunctions*) at 52-53; Cory, ITIF, *How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet”* at p. 13, Adam Snukal. New Copyright Law in Chile, ReedSmith April 27, 2010, <https://www.adlawbyrequest.com/2010/04/articles/intellectual-property/new-copyright-law-in-chile>; “22 sites blocked in Saudi Arabia over copyrights issues”, Gulf News, Saudi Arabia, April 3, 2014, <http://gulfnews.com/news/gulf/saudi-arabia/22-sites-blocked-in-saudi-arabia-over-copyrights-issues-1.1313281>.

¹⁰ Jo Oliver and Elena Blobel, “Website Blocking injunctions – A Decade of Development”, in Jacques de Werra (Ed) et al, *Droit d’auteur 4.0*, Schulthess Verlag (2018) (“*Oliver Website Blocking injunctions*”) at 32-42, 52-53. According to this article, website blocking in Mexico is limited to operators of targeted websites that have a physical address in Mexico. The same may be true in Brazil. See also, the decisions referred to below summarizing injunctions that have been granted around the world.

¹¹ “Gov’t ponders site blocking to stop manga piracy” The Mainichi, March 20, 2018, <https://mainichi.jp/english/articles/20180320/p2a/00m/0na/005000c>.

¹² *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014), (“*Cartier*”) aff’d [2016] EWCA Civ 658 (06 July 2016) (“*Cartier CA*”); *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc*, [2011] EWHC 1981 (Ch) (28 July 2011); *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2012] EWHC 1152 (Ch) (02 May 2012); *EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2013] EWHC 379 (Ch) (28 February 2013); *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors*, [2013] EWHC 2058 (Ch) (16 July 2013); *The Football Association Premier League Ltd v British Telecommunications Plc & Ors*, [2017] EWHC 480 (Ch) (13 March 2017); *Paramount Home*

are many cases from other countries as well.¹⁶ As further summarized below, the overwhelming findings in the decisions around the world is that blocking order remedies are a necessary tool to address Internet piracy, do not result in over-blocking, are effective, and will not violate fundamental rights.

Geist also claims that in “those countries that have had it, the most common blocking case involves a court action targeting the Pirate Bay”. It is true that The Pirate Bay domains have been blocked more than any other websites. However, site blocking orders are commonly made in waves that target many sites and services other than The Pirate Bay.

Many other notorious piracy sites have been blocked in one or more countries internationally, including Movie4k.to, EZTV, Kickass.to, Torrentz, Torrent Hound, Putlocker, PopcornTime, and PrimeWire, among many others. For example, Kickass.to, PrimeWire, and Rar BG are blocked in each of the UK, Ireland, Australia, and Portugal.

The scope of the websites blocked internationally was commented on in the 2016 ITIF report, which notes:¹⁷

A Motion Picture Association of America report from September 2015 stated that European ISPs block more than 500 websites—238 in Italy, 135 in the United Kingdom, 41 in Denmark, 24 in Spain, 18 in France, 15 in Portugal, 13 in Belgium, 7 in Norway, and smaller totals for other countries. The actual figure is likely much higher, as some

Entertainment & Anor v British Sky Broadcasting & Ors, [2014] EWHC 937 (Ch) (18 February 2014); *Paramount Home Entertainment International Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2013] EWHC 3479 (Ch) (13 November 2013); *Twentieth Century Fox Film Corporation & Ors v British Telecommunications Plc*, [2011] EWHC 2714 (Ch) (26 October 2011); *Twentieth Century Fox Film Corporation & Ors v Sky UK Ltd & Ors*, [2015] EWHC 1082 (Ch) (28 April 2015).

¹³ *EMI Records (Ireland) Limited v Eircom PLC*, Mr. Justice Charleton, 24th day of July, 2009; *EMI Records Ireland Ltd & Ors v UPC Communications Ireland Ltd & Ors*, [2013] IEHC 274 (12 June 2013); *Sony Music Entertainment (Ireland) Limited v UPC Communications Ireland Limited*, Commercial Court Record Number: 2013/ 178 COM, December 2, 2013; *Twentieth Century Fox Film Corporation, v Eircom Limited Trading as EIR*, Commercial 2017 No. 11701 P (2018 No. 6.Com), Justice McGovern Jan 15, 2018; Davinia Brennan “Court orders ISPs to block illegal streaming websites” A&L Goodbody, April 4, 2017, <https://www.irelandip.com/2017/04/articles/copyright/court-orders-isps-block-illegal-streaming-websites/>.

¹⁴ *Roadshow Films Pty Ltd v Telstra Corporation Limited*, [2017] FCA 965 (18 August 2017); *Roadshow Films Pty Ltd v Telstra Corporation Ltd*, [2016] FCA 1503 (15 December 2016); *Universal Music Australia Pty Limited v TPG Internet Pty Ltd*, [2017] FCA 435 (28 April 2017); *Foxtel Management Pty Limited v TPG Internet Pty Ltd*, [2017] FCA 1041 (1 September 2017)

¹⁵ CJEU C-134/12 *UPC Telekabel Wien*.

¹⁶ Other European and foreign cases are referred to here. Quotations are from unofficial translations.

¹⁷ Cory, Nigel, ITIF, *How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet”*, August 2016, <http://www2.itif.org/2016-website-blocking.pdf>

countries, such as the United Kingdom, do not release specific details on which websites are being blocked, in order to not alert website operators. Furthermore, countries have recently added more sites: Portugal added over 240 between December 2015 and April 2016.

All of the above shows that website blocking is not radical or rare (much less “quite rare”). In fact, it has become an essential tool for combatting internet piracy that has been thoroughly vetted and found to be a balanced and proportionate remedy around the world.

Geist claim: Other countries don't empower government agencies to make blocking orders

Geist claims that only one country, Italy, has a site blocking regime that permits site blocking by order of a government agency. He says over and over again that Canada would be “an outlier with virtually every country that has permitted site blocking” doing so through court orders. He repeatedly says this is a “fatal flaw” in the proposal. His information, which he claims is “unequivocal”, is not accurate.

At least 7 countries that have web site blocking empower government agencies¹⁸ to do so including Italy, Greece, Portugal, Malaysia, Mexico, South Korea, and Indonesia.¹⁹ Here is some background on some of them.

Italy: Italy allows the blocking of access to copyright infringing websites through administrative order. Italian courts have held that this regime is consistent with EU law and with the Italian constitution.²⁰

Portugal: Geist disregards Portugal on the basis that it is a “voluntary” regime. However, the ISPs in Portugal do not block websites without orders. There is an MOU in Portugal between rights holders, the competent government body for cultural affairs (IGAC) and the ISPs. Under the MOU rights holders can make complaints in respect of predominantly copyright infringing

¹⁸ The term “government agency” or “administrative agency” is used in this paper to mean a body with lawful authority to make an order, other than a court, such a telecommunications or communications regulator like the Korean Communications Commission (KCC) or AGCOM, the Italian telecommunications regulator, administrative authorities such as Portugal's government body for cultural affairs (IGAC) and the Greek Copyright Organization (OPI), and ministries and government departments.

¹⁹ *Oliver Website Blocking Injunctions*. Geist excludes Indonesia and Malaysia - he is critical of the site blocking they do. He also excludes Portugal.

²⁰ Kluwer Copyright Blog, “Italian Public enforcement on online copyright infringements: AGCOM Regulation held valid by the Regional Administrative Court of Lazio (but there is still room for the CJEU)”, June 16, 2017 <http://copyrightblog.kluweriplaw.com/2017/06/16/italian-public-enforcement-online-copyright-infringements-agcom-regulation-held-valid-regional-administrative-court-lazio-still-room-cjeu/>.

sites and the IGAC then issues orders requiring ISPs to block sites. Accordingly, the legal authority to block the sites is premised on the order of the IGAC. This reflects the recognition in the EU that piracy is a problem and needs to be addressed through blocking.

Greece: Greece has established a 3-member administrative authority called the Greek Copyright Organisation (OPI). It is composed of the President of OPI, a representative from the Greek Data Protection Authority and a representative from the Greek Telecommunications & Post Commission. The Commission has the power to receive complaints and issue decisions which can include orders to take down sites hosted in Greece or blocking orders against foreign sites. Blocking access to illegal content is seen as the most appropriate and effective technical means of combatting piracy of copyright content and the means used may include IP address or domain name server (DNS) blocking.²¹

South Korea: The South Korean “Korean Communications Standards Commission” has authorized blocking of websites hosting copyright-infringing materials.²² Geist excludes South Korea on the grounds that it uses “uses censors to block access to thousands of web pages”. However, there is no good basis to exclude South Korea from the list of countries that block websites for copyright purposes using a government agency.

Mexico: The Mexican Institute of Industrial Property (IMPI) has the authority to issue orders requiring that ISPs block websites. Geist claims that the Mexican Supreme Court ruled that blocking is disproportionate. The Supreme Court decision at issue held that IMPI could block *specific* incidents of copyright infringement at mymusic.com but not the entire website as there was legal content also available at the site. The Mexican Supreme Court subsequently clarified that blocking an entire website is permissible if the “totality” – meaning substantial majority – of conduct is infringing.²³

Geist further fails to acknowledge that government agencies around the world are also given authority to block websites for other purposes. For example, France has laws allowing blocking

²¹ The IPKat, “Greece: new notice and take down administrative mechanism for online copyright cases now in force”, March 5, 2018, <http://ipkitten.blogspot.ca/2018/03/greece-new-notice-and-take-down.html>; also, for the process, <http://www.opi.gr/index.php/en/committee/request-committee>.

²² MPA, “MPA Study on Site Blocking Impact in South Korea (2016)”, http://www.mpa-i.org/wp-content/uploads/2018/01/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf

²³ Luis Schmidt, “Most Counts as Total When Blocking Websites in Mexico”, November 9, 2017 <http://www.mondaq.com/mexico/x/644646/Copyright/Most+Counts+As+Total+When+Blocking+Websites+In+Mexico> >

of suspected child pornography and terrorism websites without a court order.²⁴ Australia allows certain government agencies to block certain non-copyright content without court orders.²⁵ Although Geist says that New Zealand “does not have site blocking at all”, the Department of Internal Affairs maintains a filter blocking access to child pornography.²⁶ In Sweden, police administer a list of sites known to provide access to child pornography. Major ISPs use DNS filters to block access to these sites.²⁷ In Finland, the National Bureau of Investigation maintains a list of websites containing child pornography. ISPs voluntarily block access to these websites.²⁸ Poland and Slovakia have blocking to restrict access to unlicensed gambling sites.²⁹

Geist also claims that telecom companies from around the world oppose efforts of rights holders to obtain blocking orders. However, increasingly, ISPs do not oppose such orders knowing that courts will grant them and because they benefit from and recognize the responsibility to act cooperatively to address Internet piracy. For example, in Portugal, ISPs do not oppose orders made by the regulator under the MOU that exists in that country. ISPs in other countries frequently also do not oppose such orders. In Belgium, for example, ISPs and rights holders have started to make joint applications to courts for blocking orders. According to a recent article about a Belgium application.³⁰

“The case has been running for a year already but during a hearing before the Commercial Court of Brussels this week, Benoît Michaux, lawyer for the Belgian

²⁴ The Verge, “France can now block suspected terrorism websites without a court order”. February 9, 2015, <https://www.theverge.com/2015/2/9/8003907/france-terrorist-child-pornography-website-law-censorship>.

²⁵ Computer World, “Government releases guidelines for website-blocking power”, July 17, 2017, <https://www.computerworld.com.au/article/621872/government-releases-guidelines-website-blocking-power/>.

²⁶ Tech Liberty NZ, “Media release: NZ government now filtering Internet”, March 11, 2010, <http://techliberty.org.nz/media-release-nz-government-now-filtering-Internet/>.

²⁷ Organization for Security and Co-Operation in Europe, “Freedom of Expression on the Internet”, December 15, 2011, <https://www.osce.org/fom/80723>.

²⁸ See, TechDirt, “Finnish Court OKs Censorship Of Anti-Censorship Site”, August 30, 2013, <https://www.techdirt.com/articles/20130829/11135624352/finnish-court-oks-censorship-anti-censorship-site.shtml>.

²⁹ “Polish blacklist of gambling websites” DLA Piper, Apr. 3, 2017, <https://blogs.dlapiper.com/mediaandsport/2017/04/polish-blacklist-of-gambling-websites/>; CMS Cameron McKenna Nabarro Olswang LLP, “Slovakia cracks down on online gambling”, Aug. 23, 2017, <https://www.lexology.com/library/detail.aspx?g=b1eb402a-058f-4405-9007-b1d63c494a42>.

³⁰ Andy, “Rightsholders & Belgian ISPs Cooperate to Block 450 ‘Pirate’ Domains, Torrentfreak, March 3, 2018, <https://torrentfreak.com/rightsholders-belgian-isps-cooperate-to-block-450-pirate-domains-180303/>.

Entertainment Association, explained the new approach. ‘The European legislator has put in place a mechanism that allows a national judge to request injunctions to order the providers to block access to the websites in question’, Michaux said. After being presented to the Court, the list of sites and domains will be assessed to determine whether they’re acting illegally. Michaux said that the parties have settled on a common approach and have been able to identify ‘reasonable measures’ that can be ordered by the Court that are consistent with case law of the European Court of Justice. ‘his joint request is a little unusual, things are changing, there is a certain maturation of minds, we realize, from all sides, that we must tackle the problem of piracy by blocking measures. There is a common vision on what to do and how to handle piracy,’ he said.”

It is also now common for blocking orders to be unopposed in the UK and such orders have also gone unopposed in Ireland.³¹ For example, in the Irish *Twentieth Century Fox, v Eircom* case,³² the rightholders and ISPs reached a detailed agreement on the sites to be blocked, the technical blocking measures to be adopted by each ISP, the protocol for determining what new IP addresses, domain names, and URLs could be added to block the target piracy sites, and to vary the order to address unanticipated difficulties and changes in circumstances. Following a request from the Danish Ministry of Culture and as part of a number of measures introduced to reduce the scope of rights infringements on the Internet, the members of the Telecommunications Industry Association in Denmark adopted an industry code of conduct under which ISPs voluntarily block a site if another ISP has been ordered to block it.³³

Geist claim: blocking orders must be made by courts

Geist argues that the FairPlay proposal is “fatally flawed” because the blocking orders would not be made by a court. His argument in his primary post on this issue (that Canada would be a virtual outlier if it adopted this process) rests almost entirely on his (incorrect) information about the number of countries that rely on government agencies to make blocking orders around the world.³⁴

³¹ *EMI Records Ireland Ltd & Ors v UPC Communications Ireland Ltd & Ors*, [2013] IEHC 274 (12 June 2013); *Twentieth Century Fox Film Corporation, v Eircom Limited Trading as EIR, Commercial*, 2017 No. 11701 P (2018 No. 6.Com), Justice McGovern, Jan. 15, 2018.

³² *ibid*

³³ “Telecommunications Industry Association in Denmark: Code of Conduct for handling decisions by the courts of law or authorities concerning blocking of websites due to rights infringements” 24 Sept. 2014.

³⁴ Michael Geist “The Case Against the Bell Coalition’s Website Blocking Plan, Part 4: Absence of Court Orders Would Put Canada At Odds With Almost Everyone”, February 15, 2018, <http://www.michaelgeist.ca/2018/02/case-bell-coalitions-website-blocking-plan-part-4-absence-court-orders-put-canada-odds-almost-everyone/> .

It is telling that his “court versus government agency” criticism is made on an “outlier argument”. In the past, he has argued against Canada adopting international norms related to copyright, instead arguing for “made in Canada” solutions, or relying on outlier countries as models for Canadian copyright reforms. For example, during the copyright reform process he argued that Canada should not adopt a notice and takedown system, even though that is the international standard. He argued for notice and notice, even though no other country had adopted that instead of notice and take-down. He argued that Canada should adopt watered down prohibitions against circumventing technological measures that no other country had adopted and relied on the laws in Switzerland that are regarded as being an international outlier. Further, he argued for a new user generated content (UGC) exception to copyright infringement that no other country in the world has.³⁵ More recently, he appeared before a Senate Committee and defended Canada’s “more innovative provisions” and argued we should try and export them internationally.³⁶

In any event, his argument that site blocking orders must be made by court orders as a matter of Canadian law is simply wrong. It is, as I show below, also not supported by international norms or human rights concerns.

Geist’s claim entirely fails to take into account the Canadian telecommunications framework, the status of the CRTC as having the powers of a court of superior jurisdiction, that blocking orders are subject to appeals and judicial reviews, and the well-established caselaw in Canada that confirms that decisions affecting fundamental freedoms can be lawfully made by government agencies.

Geist contends that the proposal is flawed without even considering the provisions of the *Telecommunications Act*. As Geist admits, Section 36 of the Act, has been interpreted by CRTC to give it the authority to approve website blocking. That provision is complimented by

³⁵ See, “Michael Geist Bill C-32: My Perspective on the Key Issues“, Sept. 21, 2010, <http://www.michaelgeist.ca/2010/09/c-32-perspective-on-key-issues/>; Barry Sookman “An FAQ on TPMs, Copyright and Bill C-32”, Dec. 14, 2010, <http://www.barrysookman.com/2010/12/14/an-faq-on-tpms-copyright-and-bill-c-32/>.; Barry Sookman “Change and the Copyright Modernization Act” Nov 7, 2012, <http://www.barrysookman.com/2012/11/07/change-and-the-copyright-modernization-act/>.

³⁶ Michael Geist “Canadian Copyright Diplomacy: My Appearance before the Senate Standing Committee on Foreign Affairs” Feb 7, 2018, <http://www.michaelgeist.ca/2018/02/canadian-copyright-diplomacy-appearance-senate-standing-committee-foreign-affairs/>.

other provisions of the Act that give it the jurisdiction to order ISPs to block websites.³⁷ Section 36 states:

Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.

This section has been interpreted by the CRTC as exclusively providing it with the power to approve blocking orders against ISPs.³⁸

Although Geist argues that only courts can make blocking orders because they might affect freedom of speech rights, he fails to consider that Parliament has conferred on the CRTC the powers of courts needed to protect fundamental rights and freedoms.

The CRTC is a tribunal within the Government of Canada that is responsible for regulating and supervising Canada's communication system in the public interest. It operates under a number of legislative authorities and Acts of Parliament. These include the *Broadcasting Act*, the *Telecommunications Act*, Canada's Anti-Spam Legislation (CASL) and the *Canada Elections Act* which includes provisions establishing the Voter Contact Registry (VCR). The Commission's mandate includes promoting compliance with and enforcing legislation, regulations and rules such as the Unsolicited Telecommunications Rules, CASL, the National Do Not Call List (DNCL) and the VCR.³⁹

The CRTC has quasi-judicial powers of a superior court with respect to matters that would be relevant to its capabilities to balance the interests of promoting the objectives of the telecommunications system through blocking pirate websites and online rights of freedom of expression. For example, the Commission has the jurisdiction to make findings on questions of law and fact. It also has all of the judicial powers of a superior court with respect to the attendance and examination of witnesses; the production and examination of any document; the enforcement of its decisions; the entry on and inspection of property; and the doing of anything else necessary for the exercise of its powers and the performance of its duties. It has the power to make orders respecting any matter within the jurisdiction of the Commission. Further, a decision of the Commission may be made an order of the Federal Court or of a superior court of

³⁷ *Telecommunications Act*, SC 1993, c 38, ss. 24, 24.1, 32, 51, 61(d) and 67(1).

³⁸ Telecom Decision CRTC 2016-479, *Public Interest Advocacy Centre – Application for relief regarding section 12 of the Quebec Budget Act* Dec. 9, 2016.

³⁹ *CRTC Three-Year Plan 2017-2020*, <https://crtc.gc.ca/eng/backgrnd/plan2017/plan2017.htm>.

a province and may be enforced in the same manner as an order of that court as if it had been an order of that court on the date of the decision. The Commission may also enforce any of its decisions whether or not the decision has been made an order of a court.⁴⁰

There is also judicial oversight of the decisions of the Commission. There are direct appeals to the Federal Court of Appeal from a decision of the Commission on any question of law or of jurisdiction.⁴¹ Decisions of the CRTC are also subject to judicial review by the Federal Court of Appeal under s. 28(1) of the *Federal Courts Act*.⁴²

Geist's argument against the CRTC issuing blocking orders does not, however, appear to be tied to the capabilities, or lack thereof, of the Commission. Rather, his argument appears more bluntly to be that only courts can make orders that affect the fundamental freedom of speech rights of Canadians. However, this argument is incorrect as a matter of law.

Canadian courts have authoritatively and repeatedly concluded that administrative bodies may issue orders requiring a consideration of human rights or *Charter* values and have even gone so far as to express the opinion that they are often better qualified to make these determinations because of their domain expertise. The Supreme Court of Canada decision in *Doré v. Barreau du Québec*, [2012] 1 SCR 395 is instructive:⁴³

An administrative decision-maker exercising a discretionary power under his or her home statute, has, by virtue of expertise and specialization, particular familiarity with the competing considerations at play in weighing *Charter* values. As the Court explained in *Douglas/Kwantlen Faculty Assn. v. Douglas College*, 1990 CanLII 63 (SCC), [1990] 3 S.C.R. 570, adopting the observations of Prof. Danielle Pinard:

[translation] . . . administrative tribunals have the skills, expertise and knowledge in a particular area which can with advantage be used to ensure the primacy of the Constitution. Their privileged situation as regards the appreciation of the relevant facts enables them to develop a functional approach to rights and freedoms as well as to general constitutional precepts.

(p. 605, citing “Le pouvoir des tribunaux administratifs québécois de refuser de donner effet à des textes qu’ils jugent inconstitutionnels” (1987-88), *McGill L.J.* 170, at pp. 173-74.)

This case, among others, reflected the increasing recognition by this Court of the distinct advantage that administrative bodies have in applying the *Charter* to a specific set of

⁴⁰ *Telecommunications Act*, SC 1993, c 38, Part IV.

⁴¹ *Ibid.*

⁴² *Federal Courts Act*, RSC 1985, c F-7, s. 28(1)(c).

⁴³ *Doré v. Barreau du Québec*, [2012] 1 SCR 395, 2012 SCC 12.

facts and in the context of their enabling legislation (see *Conway*, at paras. 79-80). As Major J. noted in dissent in *Mooring v. Canada (National Parole Board)*, 1996 CanLII 254 (SCC), [1996] 1 S.C.R. 75, tailoring the *Charter* to a specific situation “is more suited to a tribunal’s special role in determining rights on a case by case basis in the tribunal’s area of expertise” (para. 64; see also *C.U.P.E.*, at pp. 235-36).

Administrative bodies in Canada can, and do, make decisions with important consequences on human rights including decisions on deportations and refugee applications,⁴⁴ and determinations that human rights have or have not been violated.⁴⁵

The CRTC makes decisions that affect or limit freedom of speech rights of Canadians. A recent case in point is Canada’s Anti-Spam Law (CASL). CASL significantly impairs the freedoms of speech of Canadians, arguably to a much greater degree than blocking orders against websites that blatantly, overwhelmingly, or structurally engage in piracy ever could.⁴⁶ It is enforced by the CRTC which has the powers to order payment of significant administrative monetary penalties (AMPs) and to issue injunctions restraining the transmission of commercial electronic messages that contain speech protected by the *Charter of Rights and Freedoms*.

Recently, CASL was challenged on, *inter alia*, freedom of speech grounds. Geist, a staunch defender of CASL,⁴⁷ filed a report supporting the anti-spam regime. Yet, while he now argues that the CRTC cannot make orders that affect freedoms of speech of Canadians, when defending CASL in legal proceedings to attack its constitutionality, he did not claim that the CASL regime was fatally flawed because the CRTC was given the authority to make critical decisions affecting the freedoms of speech of Canadians. The CRTC concluded that while CASL did infringe the freedom of speech *Charter* rights of Canadians, the restrictions were reasonable and were thus constitutional.⁴⁸

If Geist is right that the CRTC does not have the authority to make orders affecting the freedom of speech of Canadians, then it is likely that CASL and other regimes administered by the CRTC such as the regulation of broadcasting and broadcasting undertakings under the *Broadcasting*

⁴⁴ Immigration and Refugee Board of Canada, <http://www.irb-cisr.gc.ca/Eng/Pages/index.aspx>

⁴⁵ Canadian Human Rights Tribunal, <https://www.chrc-ccdp.gc.ca/eng/content/human-rights-in-canada>

⁴⁶ Barry Sookman “CASL: the unofficial FAQ, regulatory impact statement, and compliance guideline”, Jan 14, 2015, <http://www.barrysookman.com/2015/01/14/casl-the-unofficial-faq-regulatory-impact-statement-and-compliance-guideline/>.

⁴⁷ Barry Sookman “Michael Geist’s defense of Canada’s indefensible anti-spam law CASL”, July 14, 2014, <http://www.barrysookman.com/2014/07/14/michael-geists-defense-of-canadas-indefensible-anti-spam-law-casl/>.

⁴⁸ *Compliance and Enforcement Decision CRTC 2017-367*, Oct. 19, 2017. The decision is under appeal to the Federal Court of Appeal.

Act, the Unsolicited Telecommunications Rules and the National Do Not Call List would be subject to the same frailty and would similarly be “fatally flawed”.

Geist also does not take into account that government agencies are given powers by legislative choice because of a specialization they have or can develop with respect to the imperatives and nuances of legislative regimes and because of the efficiencies they can bring relative to courts in specialized matters.⁴⁹ Such expertise would be useful in the establishment of an efficient blocking regime.

Geist claim: Human rights norms require courts to make blocking orders

Geist says the proposal is fatally flawed because freedom of expression on the Internet can only be limited by “a judicial determination”. His claim cannot be supported by any international laws or norms. In fact, the evidence around the world, including the sources he relies on, show the opposite is true.

Geist refers to no Canadian law to support his claim, nor does he rely on any treaty or other legally binding enactment on Canada. Rather, his argument, appears, in essence, to be that international norms require courts and not government agencies to make website blocking orders. However, to the extent that international norms on this issue form part of Canadian law, the overwhelming practice internationally is that blocking orders can be made if authorized by an order of a court or other lawful public authority.⁵⁰

⁴⁹ See *Edmonton (City) v. Edmonton East (Capilano) Shopping Centres Ltd.*, [2016] 2 S.C.R. 293: “The presumption of reasonableness is grounded in the legislature's choice to give a specialized tribunal responsibility for administering the statutory provisions, and the expertise of the tribunal in so doing. Expertise arises from the specialization of functions of administrative tribunals like the Board which have a habitual familiarity with the legislative scheme they administer: ‘... in many instances, those working day to day in the implementation of frequently complex administrative schemes have or will develop a considerable degree of expertise or field sensitivity to the imperatives and nuances of the legislative regime’ (Dunsmuir, at para. 49, quoting D. J. Mullan, ‘Establishing the Standard of Review: The Struggle for Complexity?’ (2004), 17 C.J.A.L.P. 59, at p. 93; see also *Canada (Citizenship and Immigration) v. Khosa*, 2009 SCC 12, [2009] 1 S.C.R. 339, at para. 25)”.

⁵⁰ International norms can be used to help interpret Canadian law. Of course, the weight to be afforded to international norms that have not been incorporated by statute into Canadian law will depend on all the circumstances of the case, including the legal authoritative nature of their legal source, their specificity and, in the case of customary international law, the uniformity of state practice. Further, effect cannot be given to unincorporated international norms that are inconsistent with the clear provisions of an Act of Parliament: *Rahaman v. Canada (Minister of Citizenship and Immigration)*, 2002 FCA 89.

Geist tries to make his case by relying on a one page joint declaration of Mr. LaRue, the former UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression made in January 2012. Geist states: ⁵¹

...[the] coalition proposal is inconsistent with international standards given the absence of a court order for such an “extreme measure.”

The 2012 declaration from LaRue and the IACHR-OAS Special Rapporteur on Freedom of Expression states:

all restrictions on freedom of expression, including those that affect speech on the Internet, should be clearly and precisely established by law, proportionate to the legitimate aims pursued, and based on a judicial determination in adversarial proceedings. In this regard, legislation regulating the Internet should not contain vague and sweeping definitions or disproportionately affect legitimate websites and services.

However, Geist does not refer to the much more comprehensive, 22 page, Report of the Special Rapporteur, Frank La Rue to the United Nations General Assembly on the same topic that was published in May 2011.⁵² Here Mr. LaRue, in the report to the UN, clearly states that a court order is not required:

[69] ... Any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory.

[70] ...Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences. (emphasis added)⁵³

Geist was aware of this much more thorough report yet chose not to refer to it. He published several articles on it calling it “an important new report that examines freedom of expression on

⁵¹ JOINT DECLARATION by the UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression, Jan 20, 2012, <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=888&IID=1>

⁵² General Assembly of the United Nations, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue”, May 11, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

⁵³ The declarations of Mr. LaRue have been criticized as not reflecting a balanced approach to protection of rights on the Internet and, in particular, for failing to take a balanced approach between the fundamental principles of freedom of expression and the protection of copyright which is also a human right. See, generally, IPKat, “UK response to file-sharing is still in trouble -- but should it be?”, Jun 12, 2011, <http://ipkitten.blogspot.ca/2011/06/uk-response-to-file-sharing-is-still-in.html>; Chris Castle, “Artist Rights are Human Rights”, Music, Technology, Policy, Sep. 27, 2015, <https://musictechpolicy.com/2015/09/>. Voluntary blocking of unlawful content should not necessarily be prohibited. As this is not in issue in the proposal, I do not address that issue here.

the Internet” and said that “many governments – including Canada – were quick to laud it”. He also relied on the report during the copyright reform process to oppose providing rights holders with effective means to combat illegal content on the Internet including a notice and takedown copyright regime and a graduated response regime.⁵⁴ However, although clearly relevant, he chose not to refer to it here.

Even the Electronic Frontier Foundation (“EFF”) (of which Geist is an Advisory Board member)⁵⁵ has accepted that website blocking determinations may be made by non-judicial bodies, as indicated by the EFF’s submission to the European Court of Human Rights which, relying on the May 2011 report to the UN, stated:

(ii) Any determination of what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences⁵⁶ ...

Blocking should only be ordered by a court or other independent and impartial adjudicatory body...⁵⁷ (emphasis added)

There is no question that the CRTC fulfills these requirements. Its independence has been repeatedly recognized by Canadian courts, including the Supreme Court of Canada.⁵⁸

Geist also cites a review by Stanford University students (a student policy lab practicum) of website blocking in the context of human rights:⁵⁹

⁵⁴ Michael Geist, “UN Report Says Internet Three Strikes Laws Violate International Law”, Jun. 3, 2011, <http://www.michaelgeist.ca/2011/06/un-report-on-three-strikes/>; Michael Geist, “Is Internet Access A Human Right?: The Implications for the Rules of Access”, June 21, 2011, <http://www.michaelgeist.ca/2011/06/internet-access-human-right-column/>.

⁵⁵ See, <https://www.eff.org/about/advisoryboard>.

⁵⁶ Third-Party Intervention Submissions by Article 19 and the Electronic Frontier Foundation in the European Court of Human Rights App. No. 10795/14, at paras. 16-17, <https://www.article19.org/wp-content/uploads/2017/08/170825-Submission-Kharitonov-v-Russia-A19EFF.pdf>. Quoting with approval the May 2011 Report of the UN Special Rapporteur, above.

⁵⁷ *Ibid*, at para. 36, but noting that regulatory models are more problematic than courts as government agencies are “more likely to call for measures that protect the interests they are tasked to protect, such as national security or child safety, rather than freedom of expression”.

⁵⁸ See e.g. *British Columbia Telephone Co. v. Shaw Cable Systems (B.C.) Ltd.*, [1995] 2 SCR 739, at para. 33; *Shaw Cablesystems (SMB) Ltd. et al v. MTS Communications Inc. et al*, 2006 MBCA 29, at para. 7.

⁵⁹ Stanford University Law and Policy Lab, “The ‘Right to be Forgotten’ and Blocking Orders under the American Convention: Emerging Issues in Intermediary Liability and Human Rights”, at p. 66, https://law.stanford.edu/wp-content/uploads/2017/09/The-Right-to-Be-Forgotten-and-Blocking-Orders-under-the-American-Convention-Emerging-Issues-in-Intermediary-Liability-and-Human-Rights_Sep17-.pdf [*Stanford*].

OAS countries would likely violate their human rights obligations if they held intermediaries liable for failing to block entire sites or services in cases where no court order has been issued, as this might characterize an indirect interference on freedom of expression, prohibited by Article 13, 3 of the ACHR.

For the above proposition, the Stanford students cite the *Manila Principles*, a set of guidelines produced by non-governmental activist organizations, such as the EFF, Article 19, and OpenMedia.⁶⁰

Geist, however, quotes selectively from the student paper. Elsewhere, the paper acknowledged that “site and service blocking” can be issued by administrative orders:

“SSB can be imposed based on judicial orders, administrative orders, or private requests.”⁶¹

The Stanford paper also quotes from the Council of Europe, Joint Declaration On Freedom Of Expression And “Fake News,” Disinformation And Propaganda which states that Internet intermediaries should not be liable for third party content unless they refused to obey an order of a court or other body with legal authority:⁶²

Intermediaries should never be liable for any third-party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.⁶³

Moreover, Geist’s assertion that any limitation on freedom of expression on the Internet must be made by court order is flatly contradicted by international norms as many countries including Italy, Portugal, Greece, Mexico, South Korea, Australia, France, Finland, and others permit blocking orders to be made by government agencies for copyright or other purposes as summarized above.⁶⁴

⁶⁰ ManilaPrinciples.Org, “Organizational Signatories”, <https://www.manilaprinciples.org/organization-signatories>

⁶¹ *Stanford, supra* at p. 55.

⁶² The Stanford Review acknowledges the effectiveness of blocking orders, saying that, “It is possible to bypass all three forms of blocking using circumvention tools, but the blocks are effective against the average Internet user”: *Ibid*, at p. 58.

⁶³ *Ibid*, at p. 24, quoting Council of Europe, “Joint Declaration On Freedom Of Expression And “Fake News,” Disinformation And Propaganda (2017)”, <https://www.coe.int/en/web/media-freedom/-/joint-declaration-on-freedom-of-expression-and-fake-newsdisinformation-and-propaganda>.

⁶⁴ See also, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal*

In fact, this practice is referred to in the Council of Europe's Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content. Geist quotes from the study as follows:⁶⁵

It is recalled that the courts of law are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis the issuing of blocking orders and decisions by public or private institutions other than courts of law is therefore inherently problematic from a human rights perspective. Even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued.

This passage is only one part of a much longer treatment of the issue. Geist does not quote the Council of Europe's further statement that:⁶⁶

In most states, it is courts of law which retain ultimate authority for ordering the removal and blocking of Internet content said to breach such privacy rights. This is the case for countries which operate specific rules on the removal and blocking of Internet material as well as those with no targeted legal framework, where individuals must generally rely on injunctive relief from judges under general laws. However, in countries such as France, Russia and Turkey, one finds administrative authorities with considerable powers to request the removal of material which breaches privacy rights, particularly in the field of data protection. These may even have the right, in certain circumstances, to order an Internet intermediary to remove or block access to offending material without prior judicial authority. (emphasis added)

Geist's claim that there is an international norm that website blocking can only be made by courts is also plainly contradicted by the Guideline published by the Council of Europe related to the use of Internet filters and blocking to protect freedom of expression in the EU under the *European Convention on Human Rights*.⁶⁷ The Guideline requires that member states:

Market ('Directive on electronic commerce'), Official Journal L 178, 17/07/2000 P. 0001 – 0016, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=en>, Recital (45): "The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it." Also, Articles 12(3), 13(3), 14(3).

⁶⁵ Council of Europe, "Comparative Study On Blocking, Filtering And Take-Down Of Illegal Internet Content", at p. 18, <https://edoc.coe.int/en/Internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-Internet-content-.html>, quoting OSCE, "Freedom of Expression on the Internet", (2011), <https://www.osce.org/fom/105522?download=true>.

⁶⁶ *Ibid*, at p. 16.

⁶⁷ Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (Adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies), [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&direct=true). This recommendation was also referenced in the *OSCE report* that Geist cited for the statement that only courts of law must make decisions concerning human rights.

ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;⁶⁸ (emphasis added)

Based on the forgoing, Geist's claims that the FairPlay proposal is fatally flawed for violating human rights norms because it is premised on the CRTC making the applicable orders is not correct. In fact, the forgoing shows the opposite to be true.

Geist claim: the proposal will violate Canadian net neutrality rules

Geist says that "the most audacious" assurance made by the FairPlay coalition is that "site blocking does not raise net neutrality issues". Not only does Geist fail to establish this claim, but even a cursory review of his reasons show that the opposite is true.

Geist begins his argument by stating, "that the starting principle for net neutrality is the right for users to access content and applications of their choice, blocking content is prima facie a net neutrality violation." But, as I showed in my prior post through international examples, the principle is not absolute and the "no blocking" principle does not prevent courts or other public bodies from blocking illegal content. This was recently confirmed in a statement by Minister Bains when commenting on the proposal:

Our government supports an open internet where Canadians have the ability to access the content of their choice in *accordance to Canadian laws*," said Bains, in an emailed statement to MobileSyrup. "In other words, our Government believes that *all legal content must* be treated equally by internet service providers (ISPs). That's why our government has a strong net neutrality framework in place through the Canadian Radio-television and Telecommunications Commission (CRTC)."⁶⁹ (emphasis added)

⁶⁸ Article 6(1) of the ECHR further confirms that, as in Canada under the *Charter of Rights and Freedoms*, in the EU limitations on freedoms of speech can be made by an independent tribunal. "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

⁶⁹ Sameer Chhabra, [ISED minister responds to anti-piracy group, defends net neutrality](#) MobileSyrup, Jan. 29, 2018

Geist never explains the source of his purported rule that net neutrality prevents courts or other lawful authorities from taking measures to protect the public from online illegal threats and menaces. Indeed, if such a rule existed, it would be both surprising and dangerous. It would create the incongruity that what is unlawful and can be enjoined offline cannot be enjoined online. Such a radical view of net neutrality would undermine the rule of law on the Internet and responsibility and accountability in Internet Governance. What we need is an Internet governance ecosystem that encourages freedom, responsibility, accountability and transparency, not one premised on protecting Internet criminals.⁷⁰

Geist doesn't argue that there is any international law or treaty that prevents governments from protecting the public online because of net neutrality. Accordingly, if such a rule exists internationally, it must be premised on an international norm. Leaving aside just how difficult it is to establish the existence of an international norm - it can't be established by pointing to the law of one or even several countries - Geist doesn't come close to citing anything that supports the existence of such a norm.⁷¹

In fact, Geist's own arguments on the FairPlay proposal show the opposite is true. As summarized above, Geist argued that human rights norms require website blocking to be mandated by court orders. In support of this claim he referred to the 2012 joint declaration which expressly recognizes that blocking orders may be made, although because of the brevity of the document it didn't elaborate on the issue of which bodies could make the orders as the much longer 2011 report to the UN did. The Stanford student project and the report from the

⁷⁰ See Neil Turkewitz "Internet Governance 3.0: The maturation of principles concerning Internet Governance" April 28, 2014 Music Notes Blog, <https://www.riaa.com/internet-governance-3-0-the-maturation-of-principles-concerning-internet-governance/> describing that Brazil adopted a net neutrality law that expressly preserved the ability to enforce intellectual property rights online. "First after many years of deliberation, Brazil adopted legislation on net neutrality and privacy designed to enhance security, privacy, and competition (known as Marco Civil) while simultaneously rejecting proposals that would have hindered the application of the rule of law—particularly with regard to the protection of intellectual property. Even within a highly charged political environment, the Brazilian government rejected the notion that freedom of expression and network neutrality somehow demanded that internet service providers remain blind to infringements on their networks, and ensured that ISPs retained the capacity to respond quickly when they became aware of such infringements. Brazilian President Dilma Rousseff signed the bill at the opening of the NetMundial conference, a "global multistakeholder Meeting on the Future of Internet Governance." The NETmundial conference was the first of its kind, and we are hopeful that it contributes to the evolution of the Internet governance ecosystem that encourages freedom, responsibility, accountability and transparency."

⁷¹ Proof of an International norm depends on all the circumstances of the case, including the legal authoritativeness of their legal source, their specificity and, in the case of customary international law, the uniformity of state practice: *Rahaman v. Canada (Minister of Citizenship and Immigration)*, 2002 FCA 89.

Council of Europe documents both cite numerous examples of website blocking around the world. Further, Geist admits that over 22 countries engage in website blocking for copyright purposes. The number that block for copyright and other purposes is even higher. But, it is hard to imagine that all of this legally authorized blocking could co-exist with an internationally recognized norm that prohibits this.

Further, as described above, many jurisdictions authorize web site blocking for copyright purposes using government agencies including Greece, Italy, and Portugal in the EU and South Korea, and others permit it for other purposes. These facts show, as I argued in my prior blog post responding to Geist, that net neutrality norms or principles are not absolute. Rather, they co-exist with - and do not trump – laws that permit website blocking by court or government agencies.

Geist tries to make his argument referring to the laws of a few countries. Even assuming that the laws of a few countries could establish an international norm when the practices around the world contradict it, Geist's examples contradict the existence of the norm he alleges to exist.

Geist admits that the United States is an example of a country with a net neutrality law that does "indeed limit its applicability to 'lawful content'". He contends, however, that "that rule has now been suspended", suggesting that this would undermine the precedent.

The FCC did not, however, vote to suspend or repudiate the core principles of net neutrality. Rather, it voted to reverse the 2015 Wheeler Order that Internet services were subject to "Title II" regulation under the U.S. Communications Act.⁷² The recent 2017 FCC's *Restoring Internet Freedom* order actually re-affirmed the policy that had been in effect in the United States since 2005 that the no blocking rule only applied to lawful content. The transparency (mandatory disclosure rule) adopted as part of the 2017 order only applies to "lawful content". Further, in the 2017 order the FCC expressly re-affirmed its policy with respect to the "Four Freedoms" originally adopted as policy statement in FCC 05-151. These were repeated in footnote 773 and are

the freedoms for consumers to (1) "access the lawful Internet content of their choice"; (2) "run applications and use services of their choice, subject to the needs of law enforcement"; (3) "connect their choice of legal devices that do not harm the network";

⁷² The recent FCC order is not yet effective. See, "Verizon, AT&T & Comcast Ask Congress to Make the Net Neutrality Repeal Stronger", Digital Music News, March 18, 2018, <https://www.digitalmusicnews.com/2018/03/18/net-neutrality-repeal-fcc-isp/>

and (4) “enjoy competition among network providers, application and service providers, and content providers.”⁷³ (emphasis added)

The newly enacted net neutrality law in Washington State continues to limit the rule to “lawful content”, further evidencing that the U.S. contradicts the claim to any such internationally accepted norm.⁷⁴

Geist also points to India’s net neutrality recommendations published by TRAI, India’s telecom regulator. He says that “TRAI established a limited exception for blocking unlawful content with no exception for piracy”. India, even according to Geist therefore, is an example of another country that counters his claim that there is a norm that blocking websites is *prima facie* a net neutrality violation. It goes farther as it also evidences that blocking by government orders does not violate an international net neutrality norm.

However, TRAI’s recommendations do not appear to be worded to exclude piracy. TRAI reviewed Section 69A of the *Information Technology Act, 2000* which expressly permits blocking by order of a designated government authority. That provision had been found to be constitutionally valid by the Supreme Court of India and has been used to block copyright pirate sites.⁷⁵ After review of the decision of the Supreme Court, TRAI concluded:

Accordingly, the Authority finds that any action taken by a TSP to implement any order of a court or direction issued by the Government, in accordance with law, or action taken in pursuance of any international treaty must be regarded as a valid exemption. (emphasis added).

Geist does not refer to the actual final recommendations of TRAI which appears to have created a broad exception for blocking any content (the wording appears to include infringing copyright

⁷³ FCC 17-166, adopted Dec 14, 2017, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf at paras. 207, 220.

⁷⁴ See, State of Washington, *SUBSTITUTE HOUSE BILL 2282*, http://lawfilesexxt.leg.wa.gov/biennium/2017-18/Pdf/Bills/House_Passed_Legislature/2282-S.PL.pdf which only prohibits blocking or impairing traffic to lawful content and does not prohibit “reasonable efforts by a provider of broadband Internet access service to address copyright infringement or other unlawful activity”; “Washington becomes first state to pass its own net neutrality bill”, March 6, 2018, http://myedmondsnews.com/2018/03/washington-becomes-first-state-to-pass-its-own-net-neutrality-bill/?utm_content=buffer39d74&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

⁷⁵ *Shreya Singhal vs U.O.I* on 24 March, 2015; *Data Reign*, “Department of Telecom India Blocks Vimeo, The Pirate Bay and Other Torrent Sites”, <https://www.datareign.com/department-of-telecom-india-blocks-vimeothe-pirate-bay-and-other-torrent-sites.html>

content) through “Implementation of any order of a court or direction issued by the Government, in accordance with law”.⁷⁶

Geist also refers to Europe’s net neutrality regulation.⁷⁷ He admits that the regulation permits website blocking of illegal content. EU’s law therefore also rebuts his argument that website blocking of illegal content is a *prima facie* violation of some international net neutrality norm.

He argues, however, that the regulation does not permit blocking by government agencies based on the wording of Article 3(3)(a) which states the following:

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, in order to:

(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers; (emphasis added)

Geist does not explain how Italy, Portugal or Greece could have implemented website blocking using government agencies if he was right. Nor does he explain how the clear wording of the regulation which excludes “comply with Union legislative acts, or national legislation” or “orders by courts or public authorities vested with relevant powers” means anything other than what it says. The only support for Geist’s position is his reference to a report by BEREC on the outcome of a consultation saying:

⁷⁶ See, “TRAI Recommendations On Net Neutrality”, November 28, 2017, http://www.trai.gov.in/sites/default/files/Recommendations_NN_2017_11_28.pdf: “Rule adopted: Principle of nondiscriminatory treatment” “A Licensee providing Internet Access Service shall not engage in any discriminatory treatment of content, including based on the sender or receiver, the protocols being used or the user equipment.” “The Licensee is prohibited from entering into any arrangement, agreement or contract, by whatever name called, with any person, natural or legal, that has the effect of discriminatory treatment of content. The Reasonable traffic management and other exceptions state: “Nothing contained in this provision shall restrict:…Implementation of any order of a court or direction issued by the Government, in accordance with law”. The term “Content” is defined as including “all content, applications, services and any other data, including its end-point information, which can be accessed or transmitted over the Internet.” and “Discriminatory treatment” is defined as including “any form of discrimination, restriction or interference in the treatment of content, including practices like blocking, degrading, slowing down or granting preferential speeds or treatment to any content.” I am not expressing any opinion on whether in India blocking for copyright purposes is or is not permitted, and if so, what mechanisms are available.

⁷⁷ EU Regulation 2015/2120, Nov. 25, 2015, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120>.

In assessing how to interpret the provision, BEREC, the Body of European Regulators for Electronic Communications, commented in 2016 that “these issues would require an approach based on legislation, rather than being voluntary or self-regulatory.” The emphasis on court orders or legislation – not voluntary or self-regulatory models – points to the need for due process that involves court or legislators.⁷⁸

The portion of the report quoted by Geist responded to submissions made during the consultation advocating that ISPs should be able to block content that was illegal under EU law on a voluntary or self-regulatory basis. It did not address any suggestion that ISPs should not be required to block illegal content by orders of public authorities.⁷⁹ Nevertheless, the regulation could be read to also permit blocking without any order on a voluntary basis based on the exception to “comply with Union legislative acts or national legislation”.

What is telling is that Geist does not refer to the final version of the *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*.⁸⁰ The Guideline first quotes from Recital 13 of the EU regulation (also not referred to by Geist) which says:

Recital 13 First, situations may arise in which providers of internet access services are subject to Union legislative acts, or national legislation that complies with Union law (for example, related to the lawfulness of content, applications or services, or to public safety), including criminal law, requiring, for example, blocking of specific content, applications or services. In addition, situations may arise in which those providers are subject to measures that comply with Union law, implementing or applying Union legislative acts or national legislation, such as measures of general application, court orders, decisions of public authorities vested with relevant powers, or other measures ensuring compliance with such Union legislative acts or national legislation (for example, obligations to comply with court orders or orders by public authorities requiring to block unlawful content). (emphasis added).

⁷⁸ BEREC Report on the outcome of the public consultation on draft BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality rules, Aug 30, 2016, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/6161-berec-report-on-the-outcome-of-the-public-consultation-on-draft-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.

⁷⁹ The report summed up the submission: “Article 3(3) third subparagraph Stakeholder responses... Another suggestion from some civil society respondents and ISPs was for NRAs to support ISPs blocking content recognized as illegal under Union law or national legislation (as also referred to in paragraph 81 / paragraph 78 of the draft Guidelines), on a voluntary or self-regulatory basis, making reference to Recital 13. For the specific case of child sexual abuse content, a reference to Directive 2011/92/EU of 13 December 2011 combating child sexual abuse was suggested. It was also suggested that NRAs should also support the ability of ISPs to filter spam at any time.”

⁸⁰ “BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules”, Aug. 30, 2016, http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.

The Guideline then repeated that an ISP could engage in blocking “for legal reasons, namely to comply with the legislation or measures by public authorities specified in that exception”.

Geist also claims that Canada’s net neutrality framework “was never limited in application to content that is ‘lawful’”. This is also not accurate.

Section 36 of the *Telecommunications Act*, as interpreted by the CRTC gives the CRTC the express authority to approve blocking by carriers.⁸¹ The CRTC ruled in the Quebec gambling decision that it would approve blocking illegal traffic “where it would further the telecommunications policy objectives set out in section 7 of the Act”.⁸² So interpreted, Canada’s net neutrality framework does not prevent blocking illegal traffic; it just requires CRTC approval to do so.

Geist cites the Commission’s Internet traffic management practices (ITMP) decision as authority for his position.⁸³ That decision also clearly stated that the CRTC had the authority to approve blocking of content. Thus, blocking orders are also not a *prima facie* violation of Canada’s net neutrality laws.

The Commission notes that the majority of parties are in agreement that actions by ISPs that result in outright blocking of access to content would be prohibited under section 36 unless prior approval was obtained from the Commission. The Commission finds that where an ITMP would lead to blocking the delivery of content to an end-user, it cannot be implemented without prior Commission approval.

Accordingly, the real question is not whether blocking illegal content violates Canadian net neutrality principles. It is what test will the CRTC apply in a case such as the FairPlay proposal.

Geist claims based on the ITMP decision that the CRTC would only make such an order in exceptional circumstances relying on the following passage from the decision:

Approval under section 36 would only be granted if it would further the telecommunications policy objectives set out in section 7 of the Act. Interpreted in light of these policy objectives, ITMPs that result in blocking Internet traffic would only be approved in exceptional circumstances, as they involve denying access to telecommunications services.

⁸¹ Section 36 states “Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.”

⁸² *Telecom Decision CRTC 2016-479, Public Interest Advocacy Centre – Application for relief regarding section 12 of the Quebec Budget Act*, Dec. 9, 2016

⁸³ *Telecom Regulatory Policy CRTC 2009-657*, Oct. 21, 2009.

Geist, however, argues that when the CRTC referred to exceptional circumstances it intended that test also to apply to blocking illegal content. However, that is questionable. The reference to “exceptional circumstances” used in the ITMP decision was not used in the gambling decision, which suggests that the Commission’s view is that blocking of illegal conduct would not be subject to the “exceptional circumstances” standard.

The Commission ITMP decision stated:

The Commission notes that Canadian ISPs have used certain ITMPs for the purposes of network security and integrity. Specifically, these ITMPs have been employed to protect users from network threats such as malicious software, spam, and distribution of illicit materials. In the Commission’s view, such activities are unlikely to trigger complaints or concerns under the Act and are a necessary part of an ISP’s network operations.(emphasis added)

Geist says that the reference “to illicit materials” in the CRTC decision only “refers to network threats, not the content of the materials”. That is one interpretation, but it is not the only one.

But, the real question is whether the ITMP decision should be read as Commission policy on Internet blocking of structurally infringing pirate sites. Blocking access to illegal content is not an “ITMP” *per se* and the “exceptional circumstances” test was developed for ITMPs. That decision dealt only with Internet traffic management practices such as those pertaining to managing traffic to prevent or respond to network congestion, as well as economic approaches, which link rates for Internet service to end-user consumption. The Commission was not considering its policy for blocking orders when developing the ITMP framework.

The Commission itself noted that the ITMP framework was not intended to apply to “ITMPs used only for the purpose of network security or in order to protect network integrity.”⁸⁴ The Commission also caveated its decision, noting that the ITMP framework was not intended to apply where the matter is “one of discrimination or preference”.⁸⁵ It can also be cogently argued that the framework was not developed to address the issue now before the CRTC.

⁸⁴ “The Commission is therefore not addressing, in this decision, ITMPs used only for the purpose of network security, nor those employed temporarily to address unpredictable traffic events (e.g. traffic surges due to global events and failures on part of an ISP’s network) in order to protect network integrity.”

⁸⁵ Finally, the Commission clarifies the circumstances in which an ITMP employed by an ISP would result in the carrier controlling the content or influencing the meaning or purpose of telecommunications. In these circumstances, the Commission’s prior approval would be required, pursuant to section 36 of the Act, but the Commission would not use the ITMP framework in its review, as the matter is not one of discrimination or preference.

The categorical assertion by Geist that the CRTC has decided the very issue in this case is simply not a reasonable conclusion.

Geist claim: website blocking is not effective

Geist claims that web site blocking is ineffective as an anti-piracy solution. He says this despite his own endorsement of site blocking as an anti-child pornography solution.⁸⁶

He refers to various studies, reports and cases, but many of those he cites actually support the conclusion that site blocking is an effective remedy. Geist also skips over other leading studies and court decisions from other countries that are important to assessing the viability of using web site blocking to reduce online infringements facilitated by piracy sites.

Geist refers to a November 2015 UK study by Professor Brett Danaher which examined the efficacy of a 2012 site block of the Pirate Bay and further site blocks in the UK in 2013. Geist says this study “found little impact when the Pirate Bay was blocked with authors concluding that effectiveness depended on far broader blocking efforts”. The “far broader blocking efforts” examined in the study, which Geist doesn’t elucidate, was that the further blocking of 19 piracy sites lead to a strong decrease in piracy levels and increases in the usage of paid streaming sites. According to the study:

These data show that the blocking of The Pirate Bay, one of the largest BitTorrent sites in the UK caused was associated with only a small decrease in total piracy and caused no increase in the adoption of legal distribution services for digital movies and television.... The data suggest that former Pirate Bay users merely switched to unblocked “proxy” sites that mirrored the contents of The Pirate Bay or dispersed to other filesharing websites to consume media illegally. As we will note later, paid legal streaming services were relatively nascent during this block. However, our data suggest that when nineteen major piracy websites were simultaneously blocked in October-November 2013, the results were different. Here we observed a strong decrease in total piracy levels as a result of these blocks and we also find that these blocks caused users of the blocked sites to increase their usage of paid legal streaming sites by 12%. The lightest users of the blocked sites (and thus the users least affected by the blocks, other than the control group) increased their clicks on paid streaming sites by 3.5% while the heaviest users of the blocked sites increased their paid streaming clicks by 23.6%. Thus, our results show website blocking may have a significant impact on legal consumption when multiple sites are blocked at once and when legal digital services are well-developed and convenient.⁸⁷

⁸⁶ Michael Geist, “Child Pornography Blocking Plan a Risk Worth Taking”, Dec. 4, 2016, <http://www.michaelgeist.ca/2006/12/project-cleanfeed-column/>

⁸⁷ Geist also referred to a Dutch study on blocking the Pirate Bay which found no lasting effect from only this site block. The conclusions of this study are consistent with the findings of Prof. Danaher

Professor Danaher updated his study in 2016. Geist did not refer to the publicly available and widely known updated study. This study is cited in almost all serious examinations of the effectiveness of web blocking on countering piracy. It examined the efficacy of a single UK site blocking order in 2014 that blocked 53 websites. The study found a 90% reduction in visits to those sites, a 22% decrease in total piracy, and a 6-10% increase in visits to legal streaming services.⁸⁸

Geist also did not refer to a corroborating study by Incopro of blocks of 24 linking and P2P portal sites in the UK published in November 2014 and updated in March 2015.⁸⁹ This study found that the blocking had both short and long term effectiveness in reducing usage of the blocked pirate websites.⁹⁰

referred to above. However, they in no way undermine the finding of Danaher and Incopro that the cumulative effects of blocking do result in decreased usage of piracy sites as a whole. See, Joost Poort Baywatch: “Two approaches to measure the effects of blocking access to The Pirate Bay”, Telecommunications Policy 38 (2014) 383–392, <https://staff.fnwi.uva.nl/j.j.vanderham/research/publications/1401-Baywatch.pdf>.

⁸⁸ Brett Danaher et al., “Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior”, April 19, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795. The abstract summarized the findings as follows:

Whether and how copyrights should be enforced in the digital age has become an important policy question and an important question for empirical research. In a prior study, we found that the court ordered blocking of the Pirate Bay website in the UK in April 2012 had only a small impact on total piracy and no impact on paid legal streaming, but that the blocking of 19 major piracy websites in November 2013 caused a significant decrease in total piracy and a significant increase in usage of paid legal streaming sites.

In this update, we ask whether the blocking of 53 piracy websites in the UK in November 2014 — which more than doubled the total number of sites being blocked in the country — had an impact on consumer behavior and how that impact compared to the previous blocks. We found that these blocks caused a 90% drop in visits to the blocked sites while causing no increase in usage of unblocked sites. This led to a 22% decrease in total piracy for all users affected by the blocks (or a 16% decrease across all users overall). We also found that these blocks caused a 6% increase in visits to paid legal streaming sites like Netflix and a 10% increase in videos viewed on legal ad-supported streaming sites like BBC and Channel 5.

⁸⁹ Incopro, “Site blocking efficacy study United Kingdom”, revised March 19, 2015, <http://www.incoproip.com/wp-content/uploads/2016/11/Site-Blocking-Efficacy-UK-revised-19-03-2015.pdf>.

⁹⁰ The report found that ISP site blocks had a significant impact on all blocked sites analysed for the UK, with all categories showing a significant decline in usage. On average, blocked sites in the UK lost 73.2% of their Alexa estimated usage following a site block and maintained those levels consistently over time. When compared to the global control, changes in Alexa estimated usage for blocked sites in the UK tracked lower in all categories and showed an overall decline in usage. The report concluded:

It is clear from the following graph that the UK has experienced a decrease in traffic to the blocked sites over time, in contrast to the global control. Whilst the global usage has exhibited an overall increase of 7.8% for these sites, a decrease of 22.9% can be seen for the UK overall.

Geist also refers to a study published by Incopro in May 2017 on the effectiveness of site blocking in Australia.⁹¹ The study, as Geist points out, examined both the reduction in usage of the sites blocked but also examined usage of a list of 250 unauthorized sites. He summarized the study findings saying:

Usage of the top 250 sites in Australia decreased by 4% (204,843) when comparing March 2017 to October 2016. Usage of the same sites reduced by 13% for the global (excluding Australia) group and by 10.8% for the global control group.

His summary ignores the findings in the study pertaining to the efficacy of blocks on the sites subject to the court orders or the explanation in the report for the relatively slower decline in usage of the top 250 unauthorized sites in Australia relative to global usage. A key finding in the report was:

that the blocks are having the desired impact having decreased usage of those sites in the target region by 45.7% more than they have decreased in the global control. Overall usage of the top 250 unauthorised sites has decreased by 4% in Australia and by 13% globally (excluding Australia). It is expected that the reason for this difference is that site blocking in Australia is not yet widespread enough to have an impact upon overall usage of the top 250 sites in the country, due to only five main sites having been blocked. Of these sites, one remains relatively popular in the region, whilst three were shut down. (emphasis added)

Geist also claimed that the Australia study concluded that the declines were lower than global averages because “there may have been an increase in the usage of some unblocked sites as a result of the most popular site being blocked.” While the study did suggest that there may have been an increase in the usage of unblocked sites as a result of popular sites being blocked, the study found that the reason may have been due to the fact that only 5 sites were blocked. That explanation was confirmed in the subsequent Incopro study.

The Incopro study of site blocking in Australia was followed up by a second study published in February 2018.⁹² This study was conducted following two further site blocking orders by Australian courts. The study showed both a marked decrease in usage of the sites blocked as well as an overall decrease in usage of the top 250 film and TV pirate sites accessed in

This demonstrates that site blocking has had an overall effect in decreasing the growth of sites in comparison with the rest of the world.

⁹¹ Incopro, “Report Site Blocking Efficacy: Australia”, May 2017, <http://www.incoproip.com/wp-content/uploads/2017/08/Australian-Site-Blocking-Efficacy-Report-Final-v.2.pdf>.

⁹² Incopro, “Site Blocking Efficacy – Key Findings Australia”, February 2018, https://www.creativecontentaustralia.org.au/literature_210629/2018_Research_-_Incopro_Study.

Australia. The report found that site blocking in Australia resulted in a usage reduction of 53.4% to blocked sites when comparing usage before blocking took effect. Usage decreased for each blocking wave implemented in the country. The usage of the top 50 piracy sites in Australia decreased by 35.1%. This was 25.5% further than the 10.6% in the previous report. The impact of the two August 2017 blocking injunctions was the driving force behind these changes. Overall usage of the top 250 unauthorised sites decreased by 25.4% in Australia.⁹³

Geist claimed that the second Australia Incopro study suffered “from technical shortcomings given the inability to actually track the impact of users shifting to VPNs in order to preserve their privacy and evade blocking efforts”. He does not mention that Incopro tracked the use of two kinds of proxies used to access the blocked sites: dedicated sites offering access or a mirror of a specific blocked site, and sites offering access to more than one blocked site from one place (‘multi-site proxies’). It concluded that the use of those proxies was low.

Incopro explained that it did not track “VPN and proxy services...because they allow users to access any website of their choice” and because “it cannot be definitively concluded that they are being used to access unauthorised sites”. Geist provides no evidence to suggest that had VPNs and proxy services been measured that the results of the study would have been materially different. It is true that some individuals may have the technical expertise and be willing to expend the time and effort to bypass a site block using a proxy service. However, the authorities have observed that many users will not have the expertise or be willing to expend the time or money to use them.⁹⁴

Geist also did not refer to other well-known publicly available studies that also demonstrate that site blocking significantly reduces usage of blocked sites as well as overall usage of other piracy facilitating sites.

Geist did not refer to a 2016 study prepared by the MPA for the Korean Communications Standards Commission (KCSC) on the impact of three web blocking orders in South Korea.⁹⁵

⁹³ Geist doesn’t dispute the overall findings in the report. Instead, he referred to a single domain of *blocked* sites containing 82 domains and referred to an online source showing that Australia remained the top traffic source for that site. He provided no explanation for this including any data showing how the actual traffic to that site changed before and after the August 2017 block of the site.

⁹⁴ Jaan Riordian, *The Liability of Internet Intermediaries* (Oxford University Press, 2016), pp 494-495, referring to various UK decisions commenting on this point. See also the cases referred to below on this point.

⁹⁵ MPA, “MPA Study on Site Blocking Impact in South Korea (2016)”, http://www.mpa-i.org/wp-content/uploads/2018/01/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf

The effects of the traffic data was clear: visits to blocked sites declined on average 90% as of three months after a block. Further, overall traffic to piracy sites (including unblocked sites) also declined. Significance testing confirmed a 15% decrease in total piracy visits.

Geist also didn't refer to the Incopro study that examined the effectiveness of the administrative site blocks implemented in Portugal published in May 2017.⁹⁶ The study found that there was an overall 69.7% drop in usage to the sites affected by the first 8 administrative blocking waves ordered in the country. The 65 blocked sites in the top 250 unauthorised sites in Portugal decreased in usage by a total of 56.6% even though they increased by 3.9% globally. Overall usage of the top 250 unauthorised sites decreased by 9.3%, even though they increased by 30.8% for the global control group clearing showing that the blocks contributed to reducing overall usage of pirate sites in Portugal.

Geist also did not refer to or consider significant data published by the IFPI in its annual Digital Musical Reports on the positive effects of site blocking on usage of pirate sites.⁹⁷

Geist referred to a 2015 Working Paper published, but not endorsed, by the European Commission. It tracked the effect of shutting down the popular German video streaming site

⁹⁶ Incopro, "Site Blocking Efficacy in Portugal (2017)", <http://www.incoproip.com/wp-content/uploads/2017/07/Site-Blocking-and-Piracy-Landscape-in-Portugal-FINAL.pdf>.

⁹⁷ Evidence of the effectiveness of site blocking has been reported by the IFPI in annual IFPI Digital Music Reports. According to the 2011 Report following The Pirate Bay being blocked in Italy, there was a 54% reduction in traffic to the site between February to October 2010; according to the 2012 Report following an order by the Antwerp Court of Appeal requiring 2 Belgian ISPs to block The Pirate Bay, there was an 84% reduction in site traffic between August and November 2011. Traffic to The Pirate Bay in Italy was still down by 74% following the site being blocked by Italian ISPs in February 2010. Further, following BTJunkie being blocked in Italy in April 2011, there was an 80% reduction in traffic to the site; according to the 2013 Report around 6.6 million Dutch Internet users were using unlicensed services in the Netherlands in January 2012. However, following the closure of MegaUpload and The Pirate Bay being blocked, this fell by 4% to 6.1 million by December 2012. Additionally, after ISPs in the Netherlands, Belgium, Finland, Italy and the UK were ordered to block The Pirate Bay, usage level of this site fell 69%. In contrast, countries without the block saw traffic increase by 45%; according to the 2014 Report BitTorrent usage was down 11% across EU countries with website blocking vs an increase of 15% in BitTorrent usage in EU countries without blocks. The effect was particularly noticeable in the UK and Italy where the highest number of sites have been blocked. In Italy, BitTorrent traffic declined 13% in 2013 and in the UK, traffic declined by 20% in 2013; according to the 2015 Report since The Pirate Bay and numerous other sites have been blocked in the UK there had been a 45 per cent decline (from 20.4m in April 2012 to 11.2m in April 2014) in visitors from the UK to all BitTorrent sites, whether blocked by ISPs or not. In Italy, where courts have ordered the blocking of 24 BitTorrent sites, there has been a decline of 25.6 per cent in the number of overall BitTorrent downloads in the country in the two years from January 2013. See www.ifpi.org/content/library/dmr2011.pdf, www.ifpi.org/content/library/dmr2012.pdf, www.ifpi.org/content/library/dmr2013.pdf, <http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf>, <http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf>

Kino.to and found only short-lived reductions in piracy levels as users gravitated to other sources.⁹⁸ Geist did not, however, refer to the qualifications in the report including that the results might well have been different in markets where there are well developed alternatives (such as Canada).⁹⁹

In fact, Prof. Danaher showed that the qualification referenced above to be accurate in a later study that analysed the impact of the US government's shutdown of the major piracy site Megaupload.com on digital sales and rentals of movies.¹⁰⁰ The study found that the closing of this major online piracy site increased digital media sales and that Internet movie piracy displaced digital film sales. The study concluded that in the 18 weeks following the shutdown of MegaUpload, digital revenues for several movies were 6-10% higher across 12 countries, than they would have been if not for the shutdown.

Geist also relies on a decision of a Dutch appeals court made in January 2014 as an example of a decision which found website blocking to be ineffective. But, he failed to point out that the decision was reversed on this point by the Supreme Court of the Netherlands.

The 2014 decision Geist referred to lifted an order made by a District Court in 2012 that required the Dutch ISPs Ziggo and XS4ALL to block The Pirate Bay in the Netherlands. The District Court had found the order would have been effective and proportionate stating:

Finally Ziggo and XS4ALL alleged that the claimed orders are not proportionate, because they will not be effective. Ziggo and XS4ALL allege that subscribers can and will easily

⁹⁸ Institute for Prospective Technological Studies Digital Economy, "Working Paper 2015/01: Online Copyright Enforcement, Consumer Behavior, and Market Structure", https://ec.europa.eu/jrc/sites/jrcsh/files/JRC93492_Online_Copyright.pdf.

⁹⁹ "Our results have important implications for policy and must be interpreted with caution. While users of kino.to decreased their levels of piracy consumption by 30% during the four weeks following the intervention, their consumption through licensed movie platforms increased by only 2.5%...we also note that we cannot observe what kinds of offline-activities consumers turn to after the shutdown of kino.to, limiting our possibilities of measuring the full producer gains of the intervention. We also highlight that the effects of anti-piracy interventions are specific to the context in which they are implemented. In particular, it is likely that the effects of such interventions will vary in function of the licensed consumption alternatives available in the market. Because German licensed online consumption channels were scarce in 2011, consumers had only limited opportunities to switch to licensed digital consumption of movies after the shutdown of kino.to. Given the importance of licensed alternatives to reduce piracy (Danaher et al., 2010, 2013), the results of these anti-piracy interventions may well be very different in an environment with more and better licensed offers available to consumers. In particular, they may be more effective in converting consumers from unlicensed to licensed consumption." (Emphasis added)

¹⁰⁰ Brett Danaher / Michael D. Smith "Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales –September 2013", <http://www.sciencedirect.com/science/article/pii/S0167718713001288>.

circumvent the blockades, since there are several technical options to do so, such as for instance by using an anonymous web proxy provider or by virtual hosting.

In the view of the District Court the defense that a blockade is not effective and as a result disproportionate is unsuccessful. Without any doubt there will be subscribers who will (know how to) circumvent the blockades, as Ziggo and XS4ALL allege. However, this is not a sufficient ground to dismiss the claimed blockades. In any case the blockades will be an additional barrier. This already appears from the circumstance that in Italy, witness the documents submitted by Brein as are not refuted, after the access to The Pirate Bay had been blocked, in several months the number of visitors of The Pirate Bay dropped from 140,000 to less than 10,000 unique visitors a day. A similar trend can be seen with the blockade in Denmark, as Brein alleged without being refuted.¹⁰¹

The 2014 court of appeal decision Geist referred to, lifted the injunction on the basis that it was not proportionate because it was not effective.¹⁰² What Geist failed to mention is that the case was appealed to the Supreme Court of the Netherlands on two issues.¹⁰³ First, whether the court below had erred in concluding that the order was ineffective and not proportionate; secondly, whether there was a legal basis to grant an injunction in the first place.

On the first issue, the Supreme Court reversed the 2014 decision that had found the order not to be proportionate finding the court had erred in law in its assessment of the effectiveness of the injunction. According to the court:

The purpose of the action by Brein is to obtain an injunction against Ziggo is to block the access of their subscribers to TPB. The appeal court measured the effectiveness of the requested injunction against the pursued objective of Brein to completely cease (all possible) infringements of copyright of rightholders, committed with the use of the internet, or at least with use of (BitTorrent) websites. In this regard the appeal court failed to recognise that even when certain measures cannot lead to complete cessation of all copyright infringements, they can still be consistent with the condition of proportionality as meant in article 52 (1) Charter. It follows from paragraphs 62-63 of the ECJ judgment UPC Telekabel Wien after all, that the mere fact that a blocking can be circumvented, doesn't make the blocking ineffective. It is sufficient that the blocking – in so far as the blocking cannot prevent the infringements – at least makes the infringement difficult to achieve and seriously discourages internet users from committing the acts of infringement.

The judgment of the appeal court (in par 5.24) that a claim such as the one at hand could only be upheld if (all) other (relevant) BitTorrent-sites were involved in the proceedings, also demonstrates an incorrect interpretation of the law. Such a

¹⁰¹ District Court order quoted in *Stichting BREIN v Ziggo BV*, THE HAGUE COURT, Commercial Law Division, Case/Docket Number District Court C/09/535341/KG ZA 17-891, Sept 22, 2017

¹⁰² Martin Gijzemijter for Benelux “Ineffective' Pirate Bay ban lifted by Dutch court” ZDNet, January 28, 2014, <http://www.zdnet.com/article/ineffective-pirate-bay-ban-lifted-by-dutch-court/>.

¹⁰³ *Stichting BREIN v Ziggo BV*, First Chamber 14/02399 LZ/EE, Supreme Court of the Netherlands, 13 November 2015, quoted paragraphs below from unofficial translation.

requirement finds no support in European and national legislation. Without further substantiation, it cannot be seen why Brein doesn't have a rightful interest in blocking one of those sites to start off with. The judgment of the appeal court that the 'step-by-step' approach advocated by Brein means the upholding of the claim would be in contradiction with the proportionality principle of article 52(1) Charter, is therefore incorrect.

Taking the above into consideration, the sections III.3-III.4 and III.10 of the plea in the main appeal succeed.

The Supreme Court referred the question as to whether there was a legal basis to make the blocking order to the European Court of Justice. Europe's top court held that there was.¹⁰⁴

Following that ruling the blocking order was re-instated in September 2017 pursuant to an interlocutory injunction by the Hague Court which found the measure to be effective and proportionate.¹⁰⁵ According to the Dutch anti-piracy group BREIN, The Pirate Bay's main domain suffered a 40 percent drop in Dutch traffic due to local ISPs blocking the torrent site following the blocking order of the Dutch court.¹⁰⁶ The Supreme Court of the Netherlands must still decide whether to make the interlocutory order final.

Geist also doesn't mention that following this decision another Dutch court made another blocking order against streaming servers making available illicit broadcasts of soccer matches, also finding such an order would be proportionate.¹⁰⁷

While Geist referred to the overruled Dutch case to make his argument that site blocking is not effective, he did not refer to the many other cases on point that also addressed the issue even though he claims to have reviewed "many of the site blocking cases from around the world".

The leading case on website blocking in the EU is the decision of the CJEU in the *UPC Telekabel* case.¹⁰⁸ The court confirmed that blocking orders meet the EU efficacy requirement. It also held they do not have to lead to a complete cessation of the infringements or that they cannot be circumvented.

¹⁰⁴ Case C-610/15 *Stichting BREIN v Ziggo BV* [EU:C:2017:99]

¹⁰⁵ *Stichting BREIN v Ziggo BV*, THE HAGUE COURT, Commercial Law Division, Case/Docket Number District Court C/09/535341/KG ZA 17-891, Sept 22, 2017.

¹⁰⁶ Kavita Iyer, "The Pirate Bay witnesses 40 percent drop in traffic in the Netherlands", TechWorm mar 4, 2018, <https://www.techworm.net/2018/03/pirate-bay-witnesses-40-percent-drop-traffic-netherlands.html>

¹⁰⁷ *The Football Association Premier League Limited v Ecatel*, ECLI: NL: RBDHA: 2018: 615, Court of The Hague, Jan 24, 2018, C / 09/485400 / HA ZA 15-36

¹⁰⁸ CJEU C-134/12, *UPC Telekabel Wien*

As regards intellectual property, it should be pointed out at the outset that it is possible that the enforcement of an injunction such as that in the main proceedings will not lead to a complete cessation of the infringements of the intellectual property right of the persons concerned.

First, as has been stated, the addressee of such an injunction has the possibility of avoiding liability, and thus of not adopting some measures that may be achievable, if those measures are not capable of being considered reasonable.

Secondly, it is possible that a means of putting a complete end to the infringements of the intellectual property right does not exist or is not in practice achievable, as a result of which some measures taken might be capable of being circumvented in one way or another.

The Court notes that there is nothing whatsoever in the wording of Article 17(2) of the Charter to suggest that the right to intellectual property is inviolable and must for that reason be absolutely protected (see, to that effect, *Scarlet Extended*, paragraph 43).

Nonetheless, the measures which are taken by the addressee of an injunction, such as that at issue in the main proceedings, when implementing that injunction must be sufficiently effective to ensure genuine protection of the fundamental right at issue, that is to say that they must have the effect of preventing unauthorized access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right.

Consequently, even though the measures taken when implementing an injunction such as that at issue in the main proceedings are not capable of leading, in some circumstances, to a complete cessation of the infringements of the intellectual property right, they cannot however be considered to be incompatible with the requirement that a fair balance be found, in accordance with Article 52(1), in fine, of the Charter, between all applicable fundamental rights, provided that (i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorized access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right.

Other European cases have also found blocking orders to be effective and proportionate. In the *Cartier* case,¹⁰⁹ Justice Arnold found that “blocking of targeted websites has proved reasonably effective in reducing use of those websites in the UK”.

In a case involving the *Premier League*,¹¹⁰ Justice Arnold issued a blocking order against streaming servers. To prevent over blocking, the court required blocking the IP address for

¹⁰⁹ *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014), affirmed [2016] EWCA Civ 658 (06 July 2016).

FirstRow's domain name (firstrow1.eu) and was satisfied that it would not result in over-blocking. The court agreed with the evidence adduced by the applicant that even though the orders were “narrow and targeted ones” the order was likely to be reasonably effective.

In another case involving the *Premier League*¹¹¹ Justice Arnold ordered ISPs to block streaming servers to prevent access to scheduled soccer matches including by individuals using ISDs. In his decision he re-iterated his opinion that such orders would substantially reduce infringements. He said:

FAPL contends that the Order will be effective and dissuasive in that it will substantially reduce infringements of FAPL's copyrights in the Works by UK consumers accessing the Target Servers. This contention is supported by a number of factors.

First, past experience suggests that blocking causes a material reduction in the number of UK users who access blocked websites: see for example the evidence reviewed in my judgment in *Cartier* at [220]-[236]. The same may be expected to be true of blocked streaming servers.

Secondly, recent academic literature supports this conclusion. For example, research by Brett Danaher, Michael Smith and Rahul Telang of the School of Information Systems, Heinz College, Carnegie Mellon University published in April 2016 (available via SSRN) concluded that blocking of 53 BitTorrent and online streaming websites as a result of orders of this Court in November 2014 reduced access to those sites by 90% from the UK, resulted in a decrease in overall piracy rates by 22% for users affected by the blocks, and increased consumption of legal content by between 6% (Netflix) and 10% (BBC and Channel 5).

Thirdly, as discussed above, blocking access to streaming servers is likely to be more effective than blocking websites which embed or link to streams from such servers both because streaming servers are the crucial link and because multiple websites typically embed or link to each server stream.

Fourthly, monitoring and blocking techniques employed by FAPL and the Defendants respectively have improved considerably since earlier blocking orders were made, in some instances because of improved automation and in other instances because of the investment of manual resources to carry out blocking at the relevant times. This makes it feasible to identify and block Target Servers much more rapidly than before, leading to the prevention of an even greater proportion of potential infringements.

Fifthly, there is reason to hope that blocking access to the Target Servers will help to educate UK consumers that accessing infringing streams is not a lawful or reliable way to access Premier League content.

¹¹⁰ *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors* [2013] EWHC 2058 (Ch) (16 July 2013)

¹¹¹ *Football Association Premier League Ltd v British Telecommunications plc*, [2017] EWHC 480 (Ch), [2017] ECC 17.

While there is always the prospect that some users and/or operators will circumvent blocking, there is no evidence to suggest that the likelihood of this occurring will be any greater in the present case than in other cases.

In the 1967 case,¹¹² a UK court made a blocking order against a series of BitTorrent sites. The court accepted evidence that such orders had been effective in the past even if they could be circumvented by users:

I would add that the Claimants' evidence on the present application includes additional support for the efficacy of such orders: using comScore data, the Claimants calculate that, on average, the number of UK visitors to Bittorrent websites which have been the subject of blocking orders has declined by 87%. No doubt some of these users are using circumvention measures which are not reflected in the comScore data, but for the reasons given elsewhere it seems clear that not all users do this.

In a recent U.K. decision, *Union Des Associations Européennes De Football v British Telecommunications Plc & Ors*,¹¹³ Justice Arnold made an injunction order on behalf of UEFA, the governing body for the association of soccer in Europe, requiring the ISP defendants to block, or at least impede, access by their customers to streaming servers which deliver infringing live streams of UEFA competition matches to UK consumers. In giving reasons for decision, Justice Arnold found the proposed order to be appropriate and proportionate. Dealing first with the need for the order to combat piracy he said:

First, the need for such orders has been emphasised by further evidence which has become available since then as to the scale of the problem of illicit streaming. By way of example, in a report entitled *Cracking Down on Digital Piracy* published by the Federation Against Copyright Theft in September 2017, the UK Intellectual Property Office was quoted as saying that it believed that, at a conservative estimate, a million set-top boxes with software added to them to facilitate illegal streaming had been sold in the UK in the last couple of years.

He then found that such orders had been effective and had achieved this without over-blocking.

Secondly, as noted in *FAPL v BT II* at [5], the evidence filed by FAPL in that case demonstrated that the order made in *FAPL v BT I* was very effective in achieving the blocking of access to the Target Servers during Premier League matches and that no evidence had been found of overblocking. The evidence filed in support of the present application is that the order made in *FAPL v BT II* has also been very effective and there is still no evidence of overblocking.

¹¹² *1967 Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3444 (Ch) (23 October 2014).

¹¹³ *Union Des Associations Européennes De Football v British Telecommunications Plc & Ors*, [2017] EWHC 3414 (Ch) (21 December 2017)

A court in Australia came to the same conclusion that a proposed blocking order would be effective without a danger of over-blocking.

I accept the applicants' submission that the orders sought would be effective at preventing a meaningful proportion of Australian users from infringing copyright via the online location in the future, without giving rise to a danger of "overblocking" legitimate websites.¹¹⁴

In Norway, a court recently granted a blocking order to prevent access to the streaming service Popcorn Time. The court noted the attraction of this kind of illegal site, the adverse effects on rights holders, and that the blocking order would be effective.

Probably the harmful effects of Popcorn Time are greater than the damaging effects of the previously blocked websites because Popcorn Time is especially user-friendly and can be used without much more technical knowledge than that needed to use the legal services...

Popcorn Time is also distinct from the earlier cases by its even greater usability. It is documented by a demonstration video that is attached to the application that the service works just like that of corresponding legal services. It is welcoming and easy to use, and the Popcorn Time application combines several different software elements which the users otherwise would have had to download and learn to use separately. Probably this is one of the reasons for the popularity of the service. The rights holders have characterised the user experience at Popcorn Time as a "Netflix experience" and this is, in the court's view, more or less right.

It is clear that so popular and user friendly pirate services have major adverse effects for the rights holders, and that their interests to a significant extent suggest that an order should be issued. Loss of illegal services will hardly lead to all users being led over on legal alternatives, but experience indicates that blocking is an effective measure that reduces illegal use. This is documented in exhibit 34 to the application.¹¹⁵

A government agency in Portugal allowed the blocking of The Pirate Bay. In doing so it reviewed the efficacy of prior blocking orders in other jurisdictions finding them to be effective, including in increasing traffic to legitimate sites (Germany) and also noted the educational benefits of web site blocking orders:

Let us now see some other relevant considerations on the issue of effectiveness. In Belgium, in September 2011, the Court of Appeal of Antwerp ordered ISPs Belgacom and Telenet to block access to the website "The Pirate Bay" by blocking the domain name service. Data from "comScore" shows that this reduced the service audience by 84% between August and November 2011. In Italy, ISPs were forced to block access to

¹¹⁴ *Universal Music Australia Pty Limited v. TPG Internet Pty Ltd*, [2017] FCA 435, (28 April 2017)

¹¹⁵ *Disney Entertainment Inc. v. Telenor Norway AS et al.*, 17-093347TVI-OTIR/05, Norway, Oslo District Court (3 November 2017)

the website “The Pirate Bay” in February 2010 (at the time, the largest torrent site in Italy), which caused the use of the service to fall dramatically – it was still at 74% in 2012 (report date in quote). In April 2011, the ISPs were also sentenced to block the website “btjunkie”, another important torrent site in Italy. The use of the service fell by 80%. In Denmark, the Supreme Court of Justice required ISPs to block access to the website “The Pirate Bay” in 2010. Blocking measures were also introduced in 2011 in Austria and Finland, requiring ISPs to block access to “The Pirate Bay” or other similar websites. In the United Kingdom, in October 2011, the Supreme Court ordered the ISP “BT” to block the unauthorised service “Newzbin2” 42. Between January 2012 and July 2013, European countries where blocking orders were determined saw the use of the website “BitTorrent” fall 11%, while European countries where this has not occurred witnessed a rise in the “BitTorrent” use by 15%....

The effect was particularly pronounced in two countries, Italy and the United Kingdom, where the largest number of illegal services was blocked. In Italy, the “BitTorrent” traffic decreased 13% in 2013 and in the United Kingdom the same traffic decreased 20% compared to the same period...

From another perspective, the side effects of the blockings cannot also be disregarded, namely the moral and pedagogical effects on users, because the fact of having their access to the works blocked will give them greater awareness of the practice – or contribution thereto – of an illegal act. Indeed, if such act is repeated freely over the years without being sanctioned and if the authorities do not take any action on the basis of the premise that it is not worth it, users will have a natural tendency to internalise the sense that the activity is legal or tolerated. A study conducted in Germany shows that the enforcement measures have been gaining acceptance among the German population, in such a way that more and more Internet users end up changing their habits of illegal downloads or streaming from legal sources. The same research shows that currently 97% of the study group realises that the download or upload of content of copyright protected works in file sharing networks is a violation of copyright law. The research also shows that awareness within the German community has increased, which is one of the effects that copyright holders aim to achieve with enforcement measures.¹¹⁶

Decisions from Courts in Denmark,¹¹⁷ Spain,¹¹⁸ and Sweden¹¹⁹ have also found that site blocking is effective.

¹¹⁶ *Associação Para a Gestão e Distribuição de Direitos et al. v. Acessos e Redes de Telecomunicações et al.*, Portugal Tribunal of Intellectual Property (24 February 2015)

¹¹⁷ *Sonofon A/S v. Aller International A/S et al.*, B-530-08, High Court of Eastern Denmark (26 November 2008) “As a starting point, blocking at DNS level is sufficiently effective. It is an established practice that the respondents cannot be referred to asserting their rights against the owners of the website.”

¹¹⁸ *Asoiacion de gestion de derechos intelectuales (AGEDI)*, E/2012/00358, Spain, Intellectual Property Commission (28 October 2014) “Moreover, the condition is met that the aforesaid execution measures have the aim of impeding, or at least, making it difficult to carry out, non-authorized access to the protected works and subject matter, and of seriously dissuading internet users resorting to the services of the relevant internet access operations from consulting this subject matter made available to them in violation of the right to intellectual property; therefore, as indicated above, blocking the specific aforesaid domain name of the piratebay group would seriously hinder access to said content.”

Courts in Europe have also observed that even if some users may find ways of circumventing blocking measures, the number who do so are limited because of the time, expertise and potential costs associated with doing so. The time and expertise acts as an impediment and the costs (such as those to subscribe to an infringing service), VPN or proxy, narrows the gap between legitimate and illegal services thus making illegal services less attractive.

In the *Newzbin2* case for example,¹²⁰ a UK court made an order to block a site that enabled users to access significant infringing content that required paying a small fee. The court found the order was likely to be effective even though some users would be able to circumvent the blocks using technical measures. According to the court:

First, it seems likely that circumvention will require many users to acquire additional expertise beyond that they presently possess. Even assuming that they all have the ability to acquire such expertise, it does not follow that they will all wish to expend the time and effort required.

Secondly, evidence filed by the Studios suggests that circumvention measures are likely to lead to slower performance and lower quality downloads, at least unless users are prepared to pay for a certain service provided by a different provider. Again, it is not necessarily the case that all users will be prepared to do this. This is not merely a question of money: there is also a potential security issue with using such services.

Thirdly, it is important not to overlook the question of economics. As I have explained above, *Newzbin2* members have to pay a subscription to use it to access content. They will also need to have a Usenet service. For the reasons Mr Hutty himself explains, they will commonly need to use a paid service. Thus they are not getting infringing content for free even as matters stand. If, in addition to paying for (a) a Usenet service and (b) *Newzbin2*, the users have to pay for (c) an additional service for circumvention purposes, then the cost differential between using *Newzbin2* and using a lawful service (such as a DVD rental service) will narrow still further. This is particularly true for less active users. The smaller the cost differential, the more likely it is that at least some users will be prepared to pay a little extra to obtain material from a legitimate service.¹²¹

¹¹⁹ *Sony Music Entertainment Sweden et al. v. B2 Bredband AB*, PMT 11706-15, Sweden, Patent and Market Appeals Court (13 February 2017) “Even though it is rather simple for the operators of the services The Pirate Bay and Swefilmer to create new web addresses etc. to provide access to the services, in the opinion of the Patent and Market Appeals Court, it is clear that an injunction nevertheless would contribute in making it more difficult to access the services.”

¹²⁰ *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981 (Ch) (28 July 2011)

¹²¹ The court also gave as a fourth reason, the reason quoted above from the *Twentieth Century Fox Film Corp & Ors v British Telecommunications* case. See also, to the same effect, *Stichting BREIN v Ziggo BV*, THE HAGUE COURT, Commercial Law Division, Case/Docket Number District Court C/09/535341/KG ZA 17-891, Sept 22, 2017 “The fact that there are methods for circumventing that blockade, e.g. through proxies, mirror sites and Virtual Private Network (VPN) connections, and still gain access to the TPB website, does not change that entirely. It goes without saying, that when the

Other courts have come to similar conclusions that the average Internet user will not try to circumvent blocking, including courts in Belgium,¹²² France¹²³ and Finland.¹²⁴ .

Geist also referred to various other documents in support of his claim, none of which detract from the strong evidence above about the effectiveness of site blocking.

He cites the UK's Ofcom's paper that stated that "any injunction scheme operated under sections 17 and 18 of the DEA is unlikely to give rise to a sufficient level of actions to have a material impact on levels of copyright infringement." This paper, however, was published in May 2010, well before the studies on the effectiveness of site blocking became available.¹²⁵

He referred to a 2015 survey published by the Council of Europe on blocking, filtering, and takedown of illegal content across the EU. The publication contained the statement Geist quoted that "blocking is not very effective in general." However, it did not refer to any study or authority on this point and appears to be a throw-away line in a study which did not endeavour

TPB website is blocked by the ISPs, it becomes less easy to reach, or in the very least access is made difficult (cf. points 62 and 63 of ECJ Telekabel Wine). Put another way, the less seasoned surfer will have more difficulty reaching the TPB website and that is sufficient for the time being. As a result, the imposing of a measure will prevent part of such circumvention (through mirror sites, for instance), because Brein can pass those websites on to the providers. Brein has moreover indicated upon being asked that it wants to address VPN providers too."

¹²² *VZW Belgian Anti-Piracy Federation v. NV Telenet et al.*, 2010/AR/2541, Belgium, Court of Appeal for Antwerp (26 Sept. 2011) "It must be assumed that the average internet user will not seek to find other ways of visiting the blocked website.")

¹²³ *Société Française du Radiotéléphone et al. v. Orange et al.*, Case No: 14/03236, France, Paris Court of First Instance (04 December 2014) "While it is correct that any blocking measures can be circumvented by some internet users, on the one hand it has not been established that the large majority of internet users, who are attached to the free-of-charge nature of communications and numerous services on the internet, have the firm intention to participate in globalised and large-scale piracy and, on the other hand, the measures sought are aimed at the majority of users who do not necessarily have the time and skills to research means of circumventing the law, which specialists find and store in their memory."

¹²⁴ *The Finnish National Group of IFPI et al. v. Anvia Oyj et al.*, Docket no. 2015/625, Finland, Mark Court (29th April 2016) "The necessity for a blocking order is not reduced by the fact that blocking measures can possibly be circumvented by some users. Under the legal praxis of the Court of Justice, measures are effective enough when they prevent unauthorised acquaintance with protected material or at least considerably hamper acquaintance and significantly reduce the appeal for internet users to acquaint themselves with material made available unlawfully. In Finland, a study has been done of changes in the numbers of users of The Pirate Bay service before the discontinuation orders granted by Helsinki District Court and after them. It has clearly emerged that the discontinuation orders have reduced the appeal of The Pirate Bay service, causing a considerable fall in the number of users."

¹²⁵ Ofcom, "'Site Blocking' to reduce online copyright infringement", https://www.ofcom.org.uk/_data/assets/pdf_file/0022/12838/1-186872101-attachment1.pdf?lang=en.

to examine or discuss the effectiveness of website blocking. It was also published before the studies on the effectiveness of site blocking.¹²⁶

Geist also referred to some information gathered by a consultant about the extent of Internet piracy in Spain (that he characterized as a “study”).¹²⁷ The document, which showed a decline of 4% in illegal usage of pirate content, did not purport to examine the effectiveness of website blocking or to compare the rates of piracy to any baseline which would enable any conclusions to be drawn. The “Observatory” however emphasized the need to improve the processes used to combat piracy in Spain. It also contained the results of a user survey which found that users believed that website blocking is the most effective means of countering illegal copyright piracy.¹²⁸

Hugh Stephens recently published an article which critically reviewed Geist’s claims that site blocking was not effective. He summed up his thinking saying:

Despite the fact there is conclusive evidence that site blocking is an effective weapon against offshore content-theft websites when applied consistently and against most of the major piracy sites, let’s revert to common sense and ask a few basic questions:

“If site blocking is as ineffective as Michael Geist claims, why would this Coalition, which includes most of the major ISPs in the country, ethnic and national broadcasters, major cinema chains, unions and sports entertainment companies, waste time and resources on what would be a quixotic journey?”

¹²⁶ Council Of Europe, “Comparative Study on blocking, filtering and take-down of illegal internet content (2015)”, <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>. The publication was prepared by the Swiss Institute of Comparative Law (SICL) and was qualified with the statement that “The opinions expressed in this document do not engage the responsibility of the Council of Europe.”

¹²⁷ La Coalicion, “Observatory 2016: Piracy down 4%”, April 25, 2017, <http://lacoalicion.es/2017/04/25/piracy-down-4/>.

¹²⁸ “The situation proves that legislative measures have a positive impact, but the results of their implementation are still insufficient, so we need more resources to be allocated and greater agility in the procedure. We are witnessing the first decrease of piracy in the last ten years, and it is an excellent opportunity to revert the enormous damage it causes to creators, to the industries, but also to employment, the public purse and to our country’s competitiveness in a global market. We want to keep up with our neighbours’ results, countries such as Italy or Portugal, and get as close as possible to the United Kingdom, France or Germany”, stated Carlota Navarrete, director of the Coalition.” The Observatory also contain the result of a survey of what users believed would best counter illegal online file sharing that stated “Most efficient measures against piracy would be, to the Internet users’ own view, blocking access to the website offering content (68%) and penalising Internet providers (61%). Following these two, the best measures to reduce infringements would be, according to consumers, imposing fines to users (53 %) and promoting social awareness campaigns against piracy (52%).”

Why all this effort from so many quarters if it is so obvious that site blocking doesn't actually work?"

In other words, "What does Michael Geist know that everyone else doesn't know?"¹²⁹

Geist claim: The proposal will lead to widespread over-blocking of legal content

Geist claims that the proposal will inherently lead to substantial over-blocking of legal content. It is somewhat ironic that Geist claims site blocking will lead to substantial over-blocking given he also argues it is ineffective. But, in any event, Geist doesn't make out his case that the proposal will necessarily lead to any substantial over-blocking of legal sites.

To make his case, he lists reported circumstances in which blocking has led to instances of temporary over-blocking. But, his conclusion that the proposal will inherently result in significant over-blocking cannot be supported by merely listing instances of reported over-blocking. Any uses of a technology can result in some unintended glitches, as anyone who has used a computer or software application knows. The probative questions, which Geist doesn't try to answer, are how frequently does site blocking result in any significant over-blocking, why the over-blocking occurred, how serious and prolonged the over-blocking lasted, whether measures can be taken to reduce or eliminate instances of over-blocking, and whether the possibility that instances might occur is a sufficient reason to reject web site blocking as a solution to the piracy problem.

The probability that a given blocking scheme will result in over-blocking varies depending on the blocking technology used and how it is deployed. The proposal does not specify how the blocks should be administered. Therefore, the CRTC would have the discretion as to which types of blocking to specify, if it decided to be prescriptive as to the methods to be used. The IPRA or the CRTC could, for example, seek assurances or impose conditions regarding the method of blocking to be employed or require assurances that if ISPs deploy IP address blocking steps are taken to ensure that non infringing sites would not be blocked.

Content blocks are generally administered by IP address, DNS (Domain Name System) or sub-domain names,¹³⁰ URL paths¹³¹ (which are used in Canada¹³² and the UK¹³³ to block child

¹²⁹ Hugh Stephens "The Effectiveness of Site Blocking: It is a Matter of Common Sense", Mar. 11, 2018, <https://hughstephensblog.net/2018/03/11/the-effectiveness-of-site-blocking-it-is-a-matter-of-common-sense/>.

¹³⁰ A DNS server translates a domain name (e.g. www.Example.com) into an IP Address. ISPs implement DNS blocking by coding their DNS servers to not resolve the blocked domain names.

¹³¹ URL path filtering blocks access to particular website paths (e.g., YouTube.com/InfringingVideo).

pornography), hybrid blocking (which employs a combination of techniques such as IP and DNS and is a standard used around the world)¹³⁴ or a hybrid of DNS and URL blocking (which was recommended by Ofcom¹³⁵).

Many of the examples of over-blocking mentioned by Geist involved blocking by IP address with no hybrid measures or other mitigating approaches. There is a known risk in using this method because websites often share IP addresses. But, over-blocking occurs only where it is impossible to determine prior to blocking whether a given IP hosts multiple websites.

Experienced rightsholders usually check to see if a target site is suitable for blocking by IP address. Many pirate sites are an appropriate target because they have dedicated IP addresses. In light of this known possible issue, evidence has been adduced in blocking cases on whether target sites share an IP address with other sites including in the UK and Australia to counter the risk of over-blocking.¹³⁶ In the recent U.K. decision, *Union Des Associations Européennes De Football v British Telecommunications Plc & Ors*,¹³⁷ Justice Arnold made an order to block illegal streaming of soccer matches. Before making the order, he reviewed two prior similar orders and found they had been effective without any evidence of over-blocking.

The issue also arose in an Austrian case in which it was argued that blocking an entire website using IP address blocking would lead to over-blocking. The court rejected the argument based on evidence that the IP address of the site was not shared with another site.¹³⁸

¹³² Cybertip.ca, “Cleanfeed Canada”, <https://www.cybertip.ca/app/en/projects-cleanfeed>

¹³³ Ofcom, “‘Site Blocking’ to reduce online copyright infringement”, https://www.ofcom.org.uk/_data/assets/pdf_file/0022/12838/1-186872101-attachment1.pdf?lang=en.ment.

¹³⁴ International Chamber of Commerce, “Roles And Responsibilities Of Intermediaries: Fighting Counterfeiting And Piracy In The Supply Chain”, at pg. 75, <https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf>.

¹³⁵ Ofcom, “‘Site Blocking’ to reduce online copyright infringement”, at pg. 41, https://www.ofcom.org.uk/_data/assets/pdf_file/0022/12838/1-186872101-attachment1.pdf?lang=en [Ofcom].

¹³⁶ *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors*, [2013] EWHC 2058 (Ch), *Roadshow Films Pty Ltd v Telstra Corporation Ltd*, [2016] FCA 1503.

¹³⁷ *Union Des Associations Européennes De Football v British Telecommunications Plc & Ors*, [2017] EWHC 3414 (Ch) (21 December 2017); See also, *Universal Music Australia Pty Limited v. TPG Internet Pty Ltd*, [2017] FCA 435, Australia, Federal Court of Australia (28 April 2017), court determining a blocking order would be effective without a risk of over-blocking.

¹³⁸ *Constantin Film Verleih GmbH v. UPC Telekabel Wien GmbH*, 4 Ob 6/12d, Austria, Supreme Court of Austria (11 May 2012). “The Plaintiffs applied, rather, for the Defendant to be ordered to deny access

Blocking orders can also mandate specific measures to mitigate the risks of over-blocking. For example, in the *Twentieth Century Fox Film v Eircom Limited Trading* case,¹³⁹ the copyright owners and ISPs reached a detailed agreement on a blocking order that was issued by an Irish court. The order contained a protocol for adding new IP addresses, domain names, and URLs to block the target pirate sites. The protocol set out relationship criteria with the target websites designed to prevent over-blocking such as that the “IP address must not be shared with other sites that are not related to the Target Websites”; the “domain name must not be shared with other sites that are not related to the Target Websites”; and that no “qualifying URL must be required to access the website, therefore the entire domain name must be dedicated to the site, not just part of the name space at that domain”. There is no reason that the IPRA and CRTC could not develop comparable means of preventing over-blocking.

The risk of over-blocking by DNS is mostly restricted to circumstances where a top-level domain name hosts both infringing and non-infringing content (e.g. YouTube.com). The issue would not arise with sites targeted by the proposal because the criteria are designed to only block whole pirate sites – the site as a whole must be “blatantly, overwhelmingly, or structurally engaged in piracy.”¹⁴⁰ If only a sub-domain met this criterion, the top-level domain would not be eligible for blocking.

URL Blocking can be performed in conjunction with DNS or IP blocking, so that only traffic directed towards a targeted domain name or IP address is directed through the “pass through” device and filtered. URL blocking requires the installation of a “pass-through” device which examines traffic to determine whether it matches a given URL. URL blocking is commonly understood to pose a low-risk of over-blocking. The 2010 Ofcom study notes that “URL blocking can be highly granular against web URLs, with low levels of over-blocking when

to the entire website for their customers. This will, in any case, only be admissible if, rather than in individual cases only, systematic and regular infringements are committed against the exclusive right of the rights holders to make particular content publicly accessible, i.e. where, in other words, there is no danger according to a realistic assessment of the blocking also preventing the access provider’s customers from obtaining content made publicly accessible in a lawful manner. This therefore rules out isolated infringements of rights by a content provider leading to general blocking by the consumers’ access providers. This requirement would be met in the case in question by virtue of the website operated at kino.to being oriented towards making protected works accessible and there thus not being any risk of general blocking also denying access to lawful content. There is no proof that, as contended by the Defendant, IP addresses of kino.to are also used by other (lawful) providers. In this respect, too, there is therefore no threat of blocking lawful content.”

¹³⁹ *Twentieth Century Fox Film Corporation, v Eircom Limited Trading as EIR, Commercial*, 2017 No. 11701 P (2018 No. 6.Com), Justice McGovern, Jan. 15, 2018

¹⁴⁰ FairPlay Coalition, CRTC Proposal, at para. 1

applied at the level of the URL.”¹⁴¹ Hybrid systems “have the advantages of IP blocking without the risks of over-blocking.”¹⁴²

Most of the incidents of over-blocking identified by Geist are related to technically flawed blocking implementations, where the court did not identify the flaws in the proposal. Arguably, a specialized tribunal like the CRTC with the assistance of a technically skilled body – with a much deeper understanding of the architecture of the Internet – could recommend what type of blocking would be appropriate or inappropriate. The combination of a specialized regulator and a technically skilled body such as the IPRA likely best minimizes the risk of over-blocking as the process will allow for the IPRA to inquire into how sites will be blocked on a case by case basis and make appropriate recommendations to the CRTC about not only what is to be blocked but by what means. Following the instance of the accidental over-blocking by the Australian securities regulator referred to by Geist, the Australian Department of Communications and the Arts published guidelines for blocking by government agencies. The guidelines recommend that “Agencies should have the requisite level of technical expertise to disrupt services under section 313(3), or procedures for drawing on the expertise of other agencies or external experts to do so. This will help ensure that requests are effective, responsible, and able to be executed appropriately.”¹⁴³

All of Geist’s claims about potential over-blocking must be assessed in a proper context. While purporting to be concerned about over-blocking, Geist completely neglects and discounts concerns about under-blocking — that is, the ready access to infringing materials made available on a mass scale by those who have built business models profiting from their illegal dissemination of infringing content.¹⁴⁴ He advances a test of the status quo – everything is fine

¹⁴¹ Ofcom, “‘Site Blocking’ to reduce online copyright infringement”, at pg. 38; see also Nigel Cory, *How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet”* (August 2016), accessed: http://www2.itif.org/2016-website-blocking.pdf?_ga=1.221850136.1203660847.1473936817,

¹⁴² UKIE, “Response to Ofcom site blocking Review”, at pg. 6, <http://ukie.org.uk/sites/default/files/UKIE%20Policy%20Paper%20-%20Response%20to%20Ofcom%20site%20blocking%20Review.pdf>

¹⁴³ “Guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services” July 17, 2017, <https://www.communications.gov.au/documents/guidelines-use-section-3133-telecommunications-act-1997-government-agencies-lawful-disruption-access>.

¹⁴⁴ See, “Good money gone bad” – Digital Thieves and the Hijacking of the Online Ad Business, A report on the Profitability of Ad-Supported Content Theft (Digital Citizens Alliance, February 2014) <http://media.digitalcitizensactionalliance.org/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf> (Research project analysed advertising-supported web sites that dealt primarily in pirated content, and found that advertising yielded enormous profits.)

with no over-blocking – with rampant unchecked piracy compared to examples of inadvertent, occasional, avoidable, and reversible over-blocking but with significant positive impacts of reducing online piracy.

Given the evidence on the effectiveness of site blocking and the attenuated risks of over-blocking, this issue is not a valid reason to oppose the proposal.

Geist claim: website blocking may violate human rights

Geist claims that the “website blocking plan... may also violate human rights norms” because “[w]ebsite blocking or other measures to limit access to the Internet raises obvious freedom of expression concerns”. He suggests that blocking orders are disproportionate on human rights grounds because of impingements on rights of freedom of expression.¹⁴⁵

Geist’s claims are not backed up by the authorities he cites, by the international practice, or the overwhelming jurisprudence contrary to his assertions which he ignores.

To make his claim, Geist refers to the Stanford student policy lab practicum which focused, in part, on the freedom of speech implications of site and service blocking (SSB) of predominantly legitimate sites.¹⁴⁶ The paper described the sites and orders it mainly dealt with as follows:

Broad SSB orders can disable entire services and websites and applications that are used to transmit ideas and expression (such as social networks, messaging apps, or apps that provide access to media and journalistic content). These orders may be issued to address pieces of unlawful content on a website or service, or serve as means to ensure enforcement of domestic regulations. In both cases, these SSB orders can be considered a severe restriction on the free flow of information and raise a number of legal and policy concerns.

This report focuses on blocks that affect entire sites and services, and not on narrower blocks targeting only individual webpages, due to the greater threat they may pose to freedom of expression and other human rights. An example of a blocking measure that affected an entire service with important consequences for the freedom to receive and impart information is the recent blocking of LinkedIn by Russian authorities, which was followed by a later order mandating the removal of the application from mobile app stores. The orders were grounded on the claim that the company failed to comply with a domestic data localization rules, which mandate that companies store users’ data within

¹⁴⁵ Geist’s argument related to the need for court orders is dealt with above.

¹⁴⁶ Stanford Law School, Law and Policy Lab, Intermediary Liability & Human Rights Policy Practicum, “The ‘Right to Be Forgotten’ and Blocking Orders under the American Convention: Emerging Issues in Intermediary Liability and Human Rights (2017)” P 56-57, https://law.stanford.edu/wp-content/uploads/2017/09/The-Right-to-Be-Forgotten_-and-Blocking-Orders-under-the-American-Convention-Emerging-Issues-in-Intermediary-Liability-and-Human-Rights_Sep17-.pdf.

the Russian territory. Similarly, in 2012 China blocked the entire New York Times website. The practice of blocking a service or application because it does not comply with local rules (in opposition to blocking orders related to unlawful content) has been observed in other countries as well, including in the OAS region. The major case in the region is, probably, the WhatsApp block in Brazil for failing to provide content of communications and other metadata to law enforcement during a local criminal investigation...(emphasis added)

Geist also refers to a 2011 joint declaration on freedom of expression and the Internet.¹⁴⁷ The declaration includes general principles including that:

Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law...

When assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests.

It also contained the statement quoted by Geist that:

Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

These general principles from the sources cited by Geist highlight the importance of freedom of expression and the obvious freedom of expression concerns of blocking entire websites devoted to legal speech.

The sources Geist relies upon also highlight that limits to freedom of expression on the Internet can be justified, are provided for by law, and protect a recognizable interest, just as is the case in the analog world. Further, they underscore the principle that freedom of expression is not an absolute principle. Rather, there is an express recognition that the principle must be balanced against other interests.

Geist, however, in claiming that the proposal may violate human rights makes no distinction between legitimate sites and those that overwhelmingly or structurally infringe copyright. He

¹⁴⁷ Frank LaRue, UN Special Rapporteur on Freedom of Opinion and Expression and others, “JOINT DECLARATION ON FREEDOM OF EXPRESSION AND THE INTERNET”, <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&IID=1>.

just refers to these quotations and implies that the same “extreme measure” concerns with these sites apply to piracy sites. This is a serious flaw in his treatment of the issue because there are fundamentally different legal and policy considerations associated with blocking legal and piracy sites.

Courts around the world recognize that freedom of speech is an important value. However, it is one that is not absolute. This is expressly recognized in Canada under the *Charter of Rights and Freedoms* which does not provide absolute freedom to disseminate unlawful materials.¹⁴⁸ Laws protecting copyright and which restrain the dissemination of copyright infringing materials have been found not to violate freedom of expression rights protected by the *Charter*.¹⁴⁹ It is not a violation of free expression to block the importation of pirated DVDs and for the same reasons it should not be a violation of free expression to block the transmission of a website full of pirated streams or copies.

This holding is consistent with laws around the world.¹⁵⁰ In the United States, for example, it is well established that laws that protect copyright do not violate First Amendment rights. Rather, protection of copyright is viewed as promoting and nurturing speech and is an engine of free expression by establishing marketable rights that supply the economic incentive to create and disseminate creative content.¹⁵¹

Although copyright is an important economic right – the most important intellectual property right that protects the creative sector – it is also recognized as being a human right internationally. It has been recognized as such, for example, in the United Nations *International Covenant on Economic, Social and Cultural Rights*¹⁵² and the United Nations *Universal Declaration of Human Rights*.¹⁵³ Courts

¹⁴⁸ *Saskatchewan (Human Rights Commission) v. Whatcott*, [2013] 1 SCR 467, at paras. 64-67.

¹⁴⁹ *Compagnie Générale des Établissements Michelin – Michelin & Cie v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, [1997] 2 F.C. 306 (Fed.T.D.), *Drolet v. Stiftung Gralsbotschaft*, 2009 FC 17, *Fraser Health Authority v. Hospital Employees’ Union*, 2003 BCSC 807, *Canwest MediaWorks Publications Inc.v.Horizon Publications Ltd.*, 2009 BCSC 391.

¹⁵⁰ See, *Television New Zealand v. Newsmonitor Services Ltd.* (1993), 27 I.P.R. 441 (H.C.N.Z.)

¹⁵¹ *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 US 539 (1985), *Eldred v. Ashcroft*, 537 US 186 (2003), *Golan v. Holder*, 132 S. Ct. 873 (2012).

¹⁵² United Nations General Assembly on December 16, 1966), <http://www.ohchr.org/EN/ProfessionalInterest/Pages/ICESCR.aspx>, Article 15(1)(c) “The States Parties to the present Covenant recognize the right of everyone... To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.”

¹⁵³ United Nations General Assembly in Paris on 10 December 1948 available @ <http://www.un.org/en/universal-declaration-human-rights/index.html>, Article 27(2) “Article 2 Everyone

in Quebec have also held that infringement of copyright may be a violation of the right of enjoyment of property protected under Articles 6 and 49 of the *Quebec Charter of Rights and Freedoms*.¹⁵⁴ In the *Cinar v Robinson* case,¹⁵⁵ the Supreme Court of Canada awarded punitive damages against several defendants finding that their infringing acts violated Robinson's rights under Sections. 1, 4 and 6 of the *Quebec Charter of Human Rights and Freedoms*.

Freedom of expression values are also enshrined under European Union law including under Article 11 of the *EU Charter of Fundamental Rights*¹⁵⁶ and Article 10(1) of the *European Convention on Human Rights*.¹⁵⁷ The European Court of Human Rights (ECHR) has acknowledged that protection of copyright is a legitimate aim that can justify an interference with freedom of expression under Article 10 of the *European Convention on Human Rights*,¹⁵⁸ and national courts throughout the EU have followed this approach.¹⁵⁹

has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.” See also, Chris Castle “Artist Rights are Human Rights”, Music, Technology, Policy, available @ <https://musictechpolicy.com/2015/09/describing-the-rights-under-other-similar-instruments>, “article 13, paragraph 2, of the American Declaration of the Rights and Duties of Man of 1948 (“Every person has the right...to the protection of his moral and material interests as regards his inventions or any literary, scientific or artistic works of which he is the author”); article 14, paragraph 1 (c), of the Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights of 1988 (the Protocol of San Salvador) (“The States Parties to this Protocol recognize the right of everyone...[t]o benefit from the protection of moral and material interests deriving from any scientific, literary or artistic production of which he is the author”).

¹⁵⁴ *Construction Denis Desjardins inc. c. Jeanson*, [2010] RJQ 1600, *France Animation v. Robinson*, 2011 QCCA 136.

¹⁵⁵ *Cinar Corporation v. Robinson*, 2013 SCC 73.

¹⁵⁶ *EU Charter of Fundamental Rights*, <http://fra.europa.eu/en/charterpedia/article/11-freedom-expression-and-information> Article 11 Freedom of expression and information states: “1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.”

¹⁵⁷ Article 10(1) states. “Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises, https://www.echr.coe.int/Documents/Convention_ENG.pdf.”

¹⁵⁸ *Ashby v France* ECHR, judgment of 10 January 2013; *Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay v Sweden - 19 February 2013)* (ECHR Case 40397/12).

¹⁵⁹ In the EU the protection of copyright is also regarded as a fundamental right that is protected under Article 17(2) of the *EU Charter of Fundamental Rights*. CJEU C-314/12 – *UPC Telekabel Wien*, C-275/06, *Promusicae v Telefónica de España*, C-324/09, *L'Oréal v eBay*, C-70/10, *Scarlet SA v SABAM*. The European Court of Justice has also ruled that restrictions on the freedom to receive information are justified where there is a need to protect intellectual property rights. *Laserdisken v. Kulturministeriet*, ECLI:EU:C:2006:549. Copyright has also been recognized as being a human right under the constitution in Ireland in a case in which a judge ruled that a graduated response regime to

A case in point involves the decision of the ECHR which ruled that jailing the founders of The Pirate Bay did not violate their rights of freedom of expression under Article 10 of the Convention.¹⁶⁰ The court noted that freedom of expression was not an absolute right and that the protection of copyrights was a reasonable limitation in a democratic society.

The test of whether an interference was necessary in a democratic society cannot be applied in absolute terms. On the contrary, the Court must take into account various factors, such as the nature of the competing interests involved and the degree to which those interests require protection in the circumstances of the case. In the present case, the Court is called upon to weigh, on the one hand, the interest of the applicants to facilitate the sharing of the information in question and, on the other, the interest in protecting the rights of the copyright-holders...

As to the weight afforded to the interest of protecting the copyright-holders, the Court would stress that intellectual property benefits from the protection afforded by Article 1 of Protocol No. 1 to the Convention (see, for example, *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, § 72, ECHR 2007-I). Moreover, it reiterates the principle that genuine, effective exercise of the rights protected by that provision does not depend merely on the State's duty not to interfere, but may require positive measures of protection (see, for example, *Öneriyıldız v. Turkey* [GC], no. 48939/99, § 134, ECHR 2004-XII). Thus, the respondent State had to balance two competing interests which were both protected by the Convention. In such a case, the State benefits from a wide margin of appreciation (*Ashby Donald and Others*, cited above, § 40; compare also to the Committee of Minister's recommendation, referred to above)...

Since the Swedish authorities were under an obligation to protect the plaintiffs' property rights in accordance with the Copyright Act and the Convention, the Court finds that there were weighty reasons for the restriction of the applicants' freedom of expression. Moreover, the Swedish courts advanced relevant and sufficient reasons to consider that the applicants' activities within the commercially run TPB amounted to criminal conduct requiring appropriate punishment. In this respect, the Court reiterates that the applicants were only convicted for materials which were copyright-protected...

In conclusion, having regard to all the circumstances of the present case, in particular the nature of the information contained in the shared material and the weighty reasons for the interference with the applicants' freedom of expression, the Court finds that the interference was "necessary in a democratic society" within the meaning of Article 10 § 2 of the Convention.

combat Internet piracy was required to protect the human rights of artists. *EMI Records & Ors -v- Eircom Ltd*, [2010] IEHC 108 case, summarized, Barry Sookman "Is graduated response necessary to protect human rights from online copyright infringement?" April 19, 2010, <http://www.barrysookman.com/2010/04/19/is-graduated-response-necessary-to-protect-human-rights-from-online-copyright-infringement/>.

¹⁶⁰ See *Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v Sweden* - 19 February 2013) (ECHR Case 40397/12).

Some opponents of website blocking claim it is censorship. However, courts around the world disagree.¹⁶¹ Some examples illustrating this are set out below.

In Argentina, a blocking order was made against The Pirate Bay. The court explained the rationale for making the order notwithstanding the constitutional protection of freedom of speech in Argentina.

"Freedom of speech is protected by the Constitution of Argentina and international treaties with constitutional hierarchy (Universal Declaration of Human Rights, Art. 19). Moreover, Law No. 26,032 states that the search for, reception and propagation of information and ideas through the Internet is covered by the constitutional guaranty protecting freedom of speech. However, it is the opinion of this Court that the admissibility of this action is in no way contrary to such directives. If it were, freedom of speech (Argentine Constitution, Art. 32) should undoubtedly be granted precedence over copyright (Argentine Constitution, Art. 17), since the former is a constitutional guarantee closer to the democratic essence of our Fundamental Law (Supreme Court, Court Decisions: 248:291)."

"Affording the protection granted by the guarantee of freedom of speech to the byte exchange regime of P2P networks, with their exchanges of chunks and metadata among users, and the assistance of trackers in the infringement of copyrights, thus elevating it to the rank of information, would amount to denigrating one of the greatest achievements of free men, elevated to the status as citizens since 1789.

Moreover, it would legitimise a voracious instrument which financially weakens publishers and exploits the works and inspiration of independent writers, journalists or bloggers working in all branches of human knowledge or research, by means or the infringement of the terms established for the exchange of ideas and information, which are the pillars of the freedom of speech."¹⁶²

There have been numerous decisions in the EU which have made blocking orders after making specific findings that such orders are proportionate and do not violate fundamental freedom of

¹⁶¹ See, Floyd Abrams, "Property theft on the Web is no less wrong" The Washington Post, Dec 9, 2011, https://www.washingtonpost.com/opinions/property-theft-on-the-web-no-less-wrong/2011/12/09/gIQAfXgDjO_story.html?utm_term=.1cf1e14c6dd9 where Floyd Abrams, one of the leading US First Amendment experts, rebutted the argument that providing a means to block rogue websites is censorship or would violate US First Amendment rights "Yet when legislation is introduced to put teeth in the effort to prevent rampant and unconstrained theft of copyrighted creative efforts, it has been denounced as creating "walled gardens patrolled by government censors." Or derided as imparting "major features" of "China's Great Firewall" to America. And accused of being "potentially politically repressive." This is not serious criticism. The proposition that efforts to enforce the Copyright Act on the Internet amount to some sort of censorship, let alone Chinese-level censorship, is not merely fanciful. It trivializes the pain inflicted by actual censorship that occurs in repressive states throughout the world. Chinese dissidents do not yearn for freedom in order to download pirated movies. Nor is it criticism that finds support in U.S. law. Infringing materials have never been protected by the First Amendment..."

¹⁶² *Capif Camara Argentina De Productores De Fonogramas et al. v The Pirate Bay*, Court of First Instance Buenos Aires, No. 67921/2013, [2013], 24.

expression values. Under EU law, courts and regulators consider whether the relief is reasonably necessary,¹⁶³ reasonably effective,¹⁶⁴ proportionate¹⁶⁵ and the likelihood of freedom of expression impacts on lawful users of the Internet.

The leading case on website blocking in the EU is the decision of the CJEU in the *UPC Telekabel (Kino.to)* case.¹⁶⁶ The court confirmed that website blocking was consistent with fundamental freedom of speech rights of Internet users as long as they are appropriately targeted at pirate sites and not broadly impacting other activity.

In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.

Courts in the EU recognize the public interest in preventing illegal conduct such as intellectual property infringement. They also recognize that site operators whose primary aim is to violate the rights of others have no expressive right that requires protection, and that Internet users have no expressive interest in accessing pirated digital goods. Nor are freedom of expression rights of Internet intermediaries violated by having to block or disable access to such sites. Blocking orders have almost invariably found not to be improper if they are targeted so that they don't unnecessarily deprive users of lawful uses of information on sites.¹⁶⁷ This approach is

¹⁶³ The question of whether the relief is reasonably necessary considers the efficiencies of seeking relief against a service provider rather than pursuing claims against many individual wrongdoers. The remedy need not be a "measure of last resort" or "indispensable" to protect a right. Rather, courts can consider if alternative measures are available that are less onerous. *Cartier CA*; *Cartier*; *Universal Music v. Telefonica Germany*, 1 ZR 174/14

¹⁶⁴ In considering the question of whether the relief is reasonably effective, courts do not require an order to eradicate the illegal behaviour. As discussed above, orders may be made even if only to dissuade some users from accessing the illegal site and even if additional Internet locations have to be added later to address efforts to circumvent the orders either by site operators or users. *Twentieth Century Fox v British Telecommunications (No. 1)* [2011] EWHC 1981 at ¶185, 192-98; *Cartier CA*; *Cartier*; *Telekabel Wien*; *Twentieth Century Fox v. British Telecommunications (No. 2)* [2011] EWHC 2714; *BAF v. Belgacom & Telenet*, (Court of Appeal, Case 2010/AR/2541); *Telenor v. IFPI Denmark* (Danish Supreme Court, case no. 153/2009).

¹⁶⁵ This involves examining whether the likely burden on the intermediary is justified by the efficacy of the remedy and the benefit to the claimant. Riordan §15.11; *Cartier*; *Cartier CA*; *Twentieth Century Fox (No. 1)*; *Telekabel Wien*.

¹⁶⁶ CJEU C-134/12 *UPC Telekabel Wien*

¹⁶⁷ Riordan, Ch. 13; *Cartier CA*, *Cartier*; *Twentieth Century Fox v. Sky UK*, [2015] EWHC 1082. *UPC Telekabel Wien* (CJEU case no. C-314/12); *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc (No. 1)*, [2011] EWHC 1981 (Ch), [2012] Bus LR 1471 (summarizing cases in the European Union). See also the decisions summarized below.

consonant with Canadian *Charter* cases, which balance the values underlying freedom of expression with other values and do not provide absolute freedom to disseminate unlawful materials.¹⁶⁸

Since Geist contends that blocking orders raise freedom of expression concerns, some of the leading authorities in the EU are summarized below. It should be recognized, however, that where blocking orders have been made, the courts had to consider all of the relevant factors before making the orders including proportionality and efficacy.

In Belgium, the Antwerp Court of Appeal, in a case regarding blocking of The Pirate Bay noted that “the ordering of the implementation of DNS blocking cannot be regarded as a restriction of freedom of expression or other fundamental rights in a manner that constitutes a violation of the *European Convention on Human Rights*.”¹⁶⁹

In France, the Tribunal de Grandes Instances de Paris (TGI) issued a judgment requiring ISPs to block access to 16 unlicensed streaming sites.¹⁷⁰ The court held that the injunction was compatible with fundamental freedom of expression rights. The Court of Appeal confirmed the findings and reiterated that the measures to block websites by ISPs do not violate rights of freedom of expression and are compliant with the principle of proportionality.¹⁷¹

Following an application filed by the film industry a court in Norway, ordered the major ISPs to block access to The Pirate Bay as well as other sites.¹⁷² The court found that an order to block access to The Pirate Bay would not conflict with freedom of speech rights under Norway’s constitution or under Article 10 of the *European Convention on Human Rights*. The infringing materials lay far beyond the core of what the freedom of speech protects and only a very small portion of the content accessed through The Pirate Bay was legal. Further, the works that were unlawfully available through The Pirate Bay were lawfully available elsewhere.

A Portuguese judgment in an action brought by Audiogest and GEDIPE (two Portuguese collective management associations) against Portuguese ISPs to block The Pirate Bay also dealt with freedom of expression rights in the blocking order context. The decision cites articles

¹⁶⁸ *Saskatchewan (Human Rights Commission) v. Whatcott*, [2013] 1 SCR 467 at paras. 64-67

¹⁶⁹ Court of Appeal Antwerp, 26 September 2011, No. 3399 Rep. 2011/8314, p. 14.

¹⁷⁰ Tribunal de Grandes Instances de Paris, 28 November 2013, No. 11/60013. .

¹⁷¹ Paris Court of Appeal judgment of 15 March 2016 [No 040/2016].

¹⁷² *Warner Bros. Entertainment Norge AS and others v Telenor Norge AS and others*, Oslo District Court, 01/09/2015, case number 15-067093TVI-OTIR/05,

6, 7, 8, 11 and 52 of the *EU Charter of Fundamental Rights* and the Council of the European Union guidelines on the conflict between freedom of expression and protecting copyright, stating that:

“any restriction must always take into account the [individual rights of freedom of expression and information], the necessity and the proportionality”.

“we cannot fail to take into account the fact the unlawfulness of the sharing and the violation of the rights of the holders of the respective rights exist, and we need a rule of law that guarantees that measures of protection of those rights are taken, although it is important that such measures are only the necessary ones and those that are less invasive as possible regarding the rights of third parties”.

“the blocking of the DNS only (domains and subdomains of the website ‘The Pirate Bay’) is shown as a much less invasive solution, and much less likely to cause damage or harm a third party, therefore being more balanced”.¹⁷³

In the UK there are numerous decisions where blocking orders have been granted and in which the courts have found such orders to be consistent with fundamental values. A leading case is *Cartier*,¹⁷⁴ a blocking case in relation to trademark infringing websites. In this case Arnold J provided guidance on the issue of balancing fundamental rights related to freedom of expression and protecting intellectual property rights.

“Where two rights, or sets of rights, are in conflict, then the conflict must be resolved by applying the principle of proportionality to each and striking a balance between them. For both reasons, it must be shown that the orders are proportionate...when assessing whether the orders are proportionate, the court is required to consider whether alternative measures are available which are less onerous.”

“As for the freedom of internet users to receive information, this plainly does not extend to a right to engage in trade mark infringement, particularly where it involves counterfeit goods. Since the Target Websites appear to be exclusively engaged in infringing commercial activity, with no lawful component to their businesses, the operators have no right which requires protection. Thus the key consideration so far as this freedom is

¹⁷³ See also, *STEF, samband tónskálda/eig flutningsréttar [Performing Rights Society of Iceland] v Fjarskipti hf.*, District Court of Reykjavik, 14. October 2014 A decision by an court in Iceland which made a blocking order against The Pirate Bay stating the following on the fundamental right to freedom of expression: “...the defendant claims that Article 59.a of the Copyright Act violates the freedom of expression cited in Article 73... the defendant’s or his customers’ freedom of expression, which includes the right to distribute and access information on the internet, is not seen to be great in relation to the plaintiff’s. In that respect it is, among other things, important to note that it is possible to access the copyrighted material with other, legal means. As such, that the stipulation in Article 59.a of the Copyright Act violates Article 73 or Article 75 of the Constitution, is dismissed. The human rights in question are allowed to be limited by law, and in the opinion of this court the requirements for limiting those constitutional rights have been fulfilled.”

¹⁷⁴ *Cartier International AG, v British Sky Broadcasting Ltd, British Telecommunications Plc*, [2014] EWHC 3354 (Ch).

concerned is the impact of the orders on users of other, lawful websites. If the orders are properly targeted, and have sufficient safeguards built into them, then that should mean that such users are not affected.”

The *Cartier* ruling was appealed by the ISPs to the Court of Appeal and was affirmed by the Court of Appeal.¹⁷⁵

As set out above, there are a plethora of decisions that have canvassed the issue of balancing freedom of expression values with the need to protect intellectual property rights. Geist claims to have reviewed “many of the site blocking cases from around the world”. Yet, in criticizing the proposal he selectively only refers to authorities from three countries, Netherlands, Germany, and Greece saying:

Courts in other countries have ruled that blocking systems may be disproportionate (Greece, the Netherlands). The Council of Europe report notes that “lower German courts have refused to follow the ECJ’s lead because of the limited effectiveness of blocking measures, which might be a problem, on the level of human rights, in terms of proportionality and transfer of judicial power to ISPs.” In light of the serious flaws with the Bell coalition website blocking proposal, a similar conclusion might well be reached in Canada.

Geist’s short paragraph suggests that blocking orders may not be available in the Netherlands or Germany on proportionality or freedom of expression grounds. Neither assertion is accurate.

I have already summarized the overruled 2014 Dutch decision Geist relies on. As I detailed above, in 2012 a Dutch District Court ordered that ISPs block The Pirate Bay finding such order to be proportionate. In 2014 a Dutch appeal court reversed that decision on efficacy grounds. In a decision not mentioned by Geist, the Supreme Court of the Netherlands overruled that decision. In September 2017 a blocking injunction was reissued on an interlocutory basis by a Dutch Court.

Geist refers again to the Netherlands arguing that website blocking may violate human rights. However, he fails to mention that the 2012 District Court decision had found the proposed blocking order to not violate freedom of speech rights, that this portion of the decision was not reversed on appeal and that the blocking order was subsequently re-instated. On the issue of freedom of speech, the District Court stated the following:¹⁷⁶

¹⁷⁵ *Cartier International AG, v British Sky Broadcasting Ltd*, [2016] EWCA Civ 658.

¹⁷⁶ 2012 District Court order quoted in *Stichting BREIN v Ziggo BV*, THE HAGUE COURT, Commercial Law Division, Case/Docket Number District Court C/09/535341/KG ZA 17-891, Sept 22, 2017

...

4.26. The right owners have a right and interest in the protection of their copyrights and neighboring rights. That the right owners incur damage by the free offer of illegal material through The Pirate Bay inter alia by the subscribers of the defendants, as Brein alleged while stating reasons, is evident in the view of the District Court. (...)

4.27. As considered above in par. 4.9 about 90% to 95% of the 3.5 million torrents which are made available through The Pirate Bay concern illegal material. When looking at what material is actually exchanged through The Pirate Bay, the rate of illegal material is even higher, because legal material is downloaded to a (much) lesser degree. The examples of legal torrents which Ziggo and XS4ALL refer to, i.e. the movie made accessible to the public through The Pirate Bay 'Die Beauty' and a music album of 'Sick of Sarah' were in any case not at all exchanged at the moment of the TNO studies through The Pirate Bay, as Brein alleged without being refuted. Furthermore Brein alleged without being refuted that torrents which refer to legal material are also provided on other websites (than The Pirate Bay). Finally, Brein alleged that the legal content – other than torrents – which is posted on The Pirate Bay itself, is restricted to information about The Pirate Bay, a webpage with 'legal issues', a 'blog', 'user conditions', and a page of 'downloads and doodles' where for instance logos of The Pirate Bay can be downloaded. Other links which are posted on the homepage of The Pirate Bay, i.e. 'Cloud, Forum, TPB-t-shirts, Bayfiles, Baywords, Baylmg, IPREDator, Follow TPB on' refer to other websites. The above is not contested by XS4ALL and Ziggo. The percentage of legal material, at least legal traffic which would be blocked by a blockade of The Pirate Bay, is therefore marginal in the view of the District Court.

4.28. Seen these circumstances the weighing of interests should be to the advantage of the right owners in the view of the District Court. That the major part of the subscribers of Ziggo and XS4ALL (presently) do not share any files through The Pirate Bay and so do not infringe the rights of the right owners, whereas they are nevertheless harmed by a blockade, as Ziggo and XS4ALL rightly allege as such, does not result into a different opinion. To the extent that such subscribers intended to start exchanging illegal material through The Pirate Bay and infringe upon doing so, this is not an interest to be respected by law. To the extent that they intended to visit The Pirate Bay without infringing, their interest is limited, seen the marginal legal offer and the option to get access to such legal offer through other websites. Such limited interest does not outbalance the protection of the parties adhered to Brein against the infringement of their rights which are extensive as to number through The Pirate Bay which can be avoided by allowing the blockade. In this the District Court further takes into account that it concerns blocking the access to a website the operators of which were already ordered by the Amsterdam District Court to render said website – and therefore including the legal content provided on it – inaccessible (see the judgment of 16 June 2010)....

...

4.40. The order should in any case also be considered necessary in a democratic society to protect the rights of others in the sense of Article 10(2) ECHR. In this respect one can confine oneself to a reference to the preceding examination of subsidiarity and proportionality, in particular the proportionality of the order in comparison with the interest of the subscribers (jur.gr. 4.23 et seq.).

Geist also doesn't mention that the Court of The Hague recently made blocking order in another case also finding such an order would not violate fundamental freedoms under EU law.¹⁷⁷

Geist's post also suggested that in Germany website blocking was not available on proportionality grounds. At one time there was uncertainty as to whether German courts had the jurisdiction to make blocking orders against ISPs. On 26 November 2015 the German Federal Court of Justice (BGH) issued two decisions on website blocking confirming that the legal basis existed.¹⁷⁸ The court also held, the proposed order to be proportionate.

The German court also found that the blocking order did not violate any right of freedom of expression protected under Article 11(1) of the *EU Charter of Fundamental Rights* and Article 5(1) of the German Constitution. The court noted that these fundamental rights required that Internet users should not be denied access to legitimate content by preventing over-blocking. The court recognized that some structurally infringing sites might contain some legal content, but held that a website block would not violate fundamental rights if only a minimal amount of legitimate content would be affected. Specifically the court said:

“The issue of legal content also being impacted (so-called "overblocking") is firstly relevant if the blocking of an IP address also prevents access to other websites which have the same IP address (c.f. Sieber/Nolde, Sperrverfügungen im Internet, 2008, p. 50). Secondly, the website at issue can contain both illegal and legal content. In the case at hand, according to the Claimants' submissions, the IP address specified in the motion is linked to four websites which all belong to the "Goldesel" service so that no other websites, which could contain legal content, would be affected by an IP block.

Unless the provider of a business model aimed at rights infringements is supposed to be able to hide behind just a small quantity of legal content, it is obvious that a block cannot be only considered permissible if solely unlawful content is provided on a website (J.B. Nordemann in Fromm/Nordemann, Urheberrecht, 11th Ed., § 97 UrhG marg. no. 170; Leistner/Grisse, GRUR 2015, 105, 108).

In the scope of the balancing of fundamental rights, the Court of Justice of the European Union also formulated the criterion of strict targeting such that the blocking measures undertaken may "not unnecessarily" deprive Internet users of the possibility of legally accessing the information available (CJEU, GRUR 2014, 468 para. 63 - UPC Telekabel; c.f. Leistner/Grisse, GRUR 2015, 105, 108). In the jurisdiction related to File-hosting, the Senate also found that it was not unreasonable to expect compliance with due diligence obligations, in the interests of effective protection of copyright, even if it could lead to a deletion of legal content in individual cases, provided the legal use of the

¹⁷⁷ *The Football Association Premier League Limited v Ecatel*, ECLI: NL: RBDHA: 2018: 615, Court of The Hague , Jan 24, 2018, C / 09/485400 / HA ZA 15-36

¹⁷⁸ FCJ judgment of 26 November 2015, Case No. I ZR 174/14 and case no. I ZR 3/14. The references to the judgment below refer to the case no. I ZR 174/14.

service provider's offering is thereby only limited to a small extent and the service provider's business model is not thereby fundamentally called into question (German Federal Court of Justice (BGH), Judgement of 12 July 2007 - I ZR 18/04, BGHZ 173, 188 para. 60 - Jugendgefährdende Medien bei eBay; BGHZ 194, 339 para. 45 - Alone in the Dark; BGH, GRUR 2013, 1030 para. 62 - File-Hosting-Dienst). Contrary to the opinion of the Appeal Court, the important factor is not the absolute number of legitimate pieces of content offered on the site at issue but the overall ratio of legal to illegal content. Furthermore, it is important to ask whether the legal content represents an insignificant amount (c.f. Leistner/Grise, GRUR 2015, 105, 108 et seq.). The fact that the Claimants base their claims only on rights in 120 music tracks but that a block would, beyond this, also cover links on the contested website to copyright protected works of third parties, rights in which the Claimants are not authorised to assert, is meaningless in this context.

On the basis of the Claimants' submissions cited by the Appeal Court, according to which legal content on the "Goldesel.to" website only accounts for a 4% share, the assumption of reasonableness of blocking measures does not fail due to the argument of legal content also being impacted."

A subsequent German court followed this case in granting a blocking order against the KINOX.TO site.¹⁷⁹ The court found that neither the pirate site nor any other person had any reasonable basis to claim that their fundamental rights of freedom of expression were violated.

The last country referred to by Geist is Greece. Greece is the outlier in the EU, being, as far as I am aware, the only jurisdiction in which blocking orders are currently not available in the courts. In light of Geist's arguments about relying on "outliers" when it comes to the need for blocking orders to be made by courts, it would be ironic for him to argue that Greece is the example to follow. Nevertheless, there has not been a blocking case in Greece since the CJEU decided the *UPC Telekabel* case in 2014, a decision that is binding on Greek courts. Further, as described above, to enable copyright holders to obtain blocking orders, Greece has now implemented a new administrative site blocking regime. As a result, Geist has not been able to point to a single country in the EU in which blocking orders cannot be obtained.

Geist claim: the proposal will lead to higher Internet access costs for all

Geist argues that the costs of implementing website blocking will result in higher Internet access costs for all consumers. However, the examples of technology costs he relies on are for

¹⁷⁹ *Constantin Film Verleih GmbH v. Vodafone Kabel Deutschland GmbH*, 7 O 17752/17, Germany, Regional Court of Munich (1 February 2018). Geist stated in a post dealing with whether ISPs generally oppose blocking orders that he had read this decision. However, he did not refer to it in his post dealing with whether blocking orders were compatible with human rights. He stated "Indeed, a review of many of the site blocking cases from around the world finds telecom companies opposing efforts to impose blocking orders. Last week, Vodafone challenged a German court order to block a streaming site, arguing that it undermines consumer rights and its freedom to operate."

different or additional technical capabilities or relate to a different context. Further, Geist does not consider the counterfactual – the increased costs associated with not having the blocking regime. Nor does he consider the proportionality of any increased costs relative to the benefits of website blocking.

Geist argues that in 2005 the government had proposed providing a grace period to ISPs with small numbers of subscribers to implement the technologies needed to comply with lawful access requirements because the “costs would have an unreasonable adverse effect on the business of the service providers”.¹⁸⁰ He doesn’t distinguish, however, between “lawful access” and “blocking” technologies. The former is expensive as it requires developing the infrastructure to allow law enforcement to intercept Internet communications pursuant to a warrant.¹⁸¹

Geist also describes the costs incurred by a number of British ISPs in developing content blocking software. For the most part, these systems did not relate solely to blocking copyright infringing websites but related to investing in blocking systems to enable them “to implement (a) the IWF blocking regime, (b) section 97A orders and (with the exception of EE) and (c) parental controls.”¹⁸²

Geist claims that “British Telecom spent over a million pounds on a DNS web-blocking system in 2012 and required more than two months of employee time on implementation.” However, the website blocking system to which he refers, Nominum, is also used to provide parental controls.¹⁸³

¹⁸⁰ Geist’s source for his second reference cites an article in which he is quoted as saying the costs of implementing lawful access technologies would put independent ISPs’ “financial survival on the line.” It World Canada, “Surveillance law could close small ISPs: Lawyer”, <https://www.itworldcanada.com/article/surveillance-law-could-close-small-isps-lawyer/45062>

¹⁸¹ Shane Snick, “Lawful Access turns up the heat on ISPs”, <https://www.itbusiness.ca/news/lawful-access-turns-up-the-heat-on-isps/1176>

¹⁸² *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3354 (Ch), <http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html>

¹⁸³ *Ibid*, at paras. 43 and 45. In 2012 BT acquired a second system called Nominum. Nominum is a DNS blocking system. Nominum is not able to block a website that shares a domain name with another website without blocking the latter. BT spent a seven figure sum purchasing this system. In addition, BT employs five people purely to support this system.... Nominum is also used to provide BT’s Parental Controls service, which was launched in December 2013. (BT also offers free downloadable Family Protection software developed in conjunction with McAfee which enables the user to protect a computer by, among other things, blocking inappropriate websites.) The Parental Controls service allows subscribers to block access to 17 broad categories of website (including pornography, gambling, social networking and games) and to block individual websites selected by

Geist claims “EE spent more than a million pounds on its web-blocking system and over 100,000 pounds every month for operations.” This system also provides much more than the blocking of piracy websites.¹⁸⁴

There was also evidence in other cases that Geist did not refer to. For example, there was evidence of blocking costs under Australia’s site blocking regime. In one case, the one-time set up costs of the ISPs were found to be, in the case of Telstra, (Aus) \$10,261 and in the case of TPG, (Aus) \$21,195.¹⁸⁵ In another case, the cost for blocking each domain name was found to be (Aus) \$50 per domain name.¹⁸⁶

Geist’s claims about potential increases in Internet costs do not consider the counter-factual, namely, would consumer costs overall be higher or lower with a website blocking regime in place than without one? If the focus of that analysis was strictly on a CRTC website blocking regime versus alternatives, it is by no means clear that blocking orders issued by courts would be any cheaper. In fact, when you add in the extensive legal fees associated with court proceedings, ISPs legal fees could well dwarf the blocking costs, especially if each application had to be on a contested basis. Moreover, rights holders would have much higher enforcement costs using the traditional court route, which would ultimately have to be passed on to consumers. The Commission could, of course, order that these costs be borne by rights holders, but so could the courts.

the users. Users can set "light", "moderate" and "strict" filter options. There is no limit on the number of individual websites that the user can choose to block.”

¹⁸⁴ *Ibid*, at para. 46 See also the following passage from ITIF “How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet”, *supra*, at pp11-12 “Detailed information on the specific costs of the various approaches and systems is unavailable, partly because this is still a relatively new policy area. In the United Kingdom, legal documents filed by lawyers representing rights holders estimated that the cost can be as high as \$18,900 per new website blocked for each ISP. UK ISPs have not publicly stated what the ongoing costs of website blocking are: What figures exist vary from a few hundred to a few thousand dollars. The cost to block the first website in the United Kingdom, for NewzBin2, was \$7,100 for the main domain and \$142 for each subsequent site (if the website operator tried to move to another site). Without providing a detailed breakdown, an Australian government estimate gave the cost per ISP to enact website blocking as \$95,000 annually. Estimates by Australian ISPs also vary—from \$36 per domain name (TPG Internet), to \$183 per site and \$29 per DNS (M2 Communications). Many countries have turned to website blocking to apply existing and new legislation to a range of legitimate public policy goals that involve the Internet. to \$7,350 in labor costs for setting up initial compliance, \$2,200 for a landing page, and \$18 per additional site (Telstra).” (footnotes omitted.)

¹⁸⁵ *Roadshow Films Pty Ltd v Telstra Corporation Ltd*, [2016] FCA 1503 (15 December 2016)

¹⁸⁶ *Universal Music Australia Pty Limited v. TPG Internet Pty Ltd*, [2017] FCA 435, (28 April 2017)

The issue of consumers' potential increase in Internet access fees, cannot be divorced however from the overall costs and economic effects associated with illegal file sharing. Illegal IPTV streaming accounts for more Internet bandwidth than illegal Bittorrent file sharing. These costs are directly or indirectly borne by consumers. Further, although Geist denies or minimizes this, piracy results in losses to producers and distributors of content – and to everyone in the legal content ecosystem. People who work in these industries are also consumers and earn less when legal markets are by-passed by illegal services. Moreover, consumers who pay for legal content end up paying more to subsidize consumers who choose to access illicit content.

We should not forget that today nearly everyone is an Internet subscriber. Viewed holistically, the proposal could actually decrease costs and/or increase welfare for consumers.

In the EU, before granting an injunction order, the courts examine whether such an order would be “proportionate”. This involves examining whether the likely burden on the intermediary is justified by the efficacy of the remedy, the benefit to the claimant, and the burdens on the intermediary.¹⁸⁷ Courts in the EU have overwhelmingly granted such orders, finding them to be proportionate. Decisions from courts finding such orders be proportionate are referred to above. Decisions in other countries contain similar findings including those from Finland,¹⁸⁸ Spain,¹⁸⁹ Norway,¹⁹⁰ Portugal,¹⁹¹ and Sweden.¹⁹²

¹⁸⁷ Riordan §15.11; *Cartier, Cartier CA ; Twentieth Century Fox (No. 1); Telekabel Wien*.

¹⁸⁸ *The Finnish National Group of IFPI et al. v. Anvia Oyj et al.*, Docket no. 2015/625, Finland, Mark Court (29th April 2016) “The teleoperators can at reasonable cost delete the domain names used by the service from their name servers and block their customers’ access to IP addresses used by the KAT site.”; *Telenor v. Aller International A/S et al.*, Case No 153/2009, Danish Supreme Court (27 May 2010) “Having been informed about the costs and inconvenience incidental to blocking at DNS level, compared with the very extensive infringement of copyrights administered by the respondents which are effected via the website www.thepiratebay.org ... the Supreme Court concurs that there are no grounds for concluding that the injunction will imply any damage or inconvenience to Telenor which are out of apparent proportion to the respondents’ interests in the issue of the injunction.”; *Elisa Oyj v. The Finnish National Group of IFPI et al.*, Decision No. 1687, Finland, Helsinki Court of Appeal (15 June 2012). “On the basis of the above and the District Court judgment, the Court of Appeal considers that the Injunction cannot be regarded as unreasonable when taking into account the rights of the person disseminating the material to the public, the rights of Elisa, and the rights of the authors. On the same basis and taking into account the evidence produced on the impact and effectiveness of IP and DNS blocking, the Court of Appeal considers that the Injunction does not contravene the principle of proportionality either.”;

¹⁸⁹ *Asociación De Gestión De Derechos Intelectuales (Agedi) v. Jazz Telecom*, Judgment No. 219/16, Spain, 2nd Commercial Court of Barcelona (27 July 2016) “the measure appears proportionate from a material and temporal point of view. It pursues non-facilitation of access to the same. Furthermore, it is appropriate to the gravity of the infringement.” “The measure blocking access to the specific domain names of the piratebay group mentioned above, and which have very high audience indices in Spain... is a measure proportional to the end being sought, which is to safeguard the rights of the

Geist claim: the proposal would increase privacy risks

Geist gives several reasons for his assertion that the FairPlay proposal would increase privacy risks for Canadians: slippery slopes, ISPs will be more likely to track the activities of users, and getting and implementing blocking orders will entail collecting personal information. He is incorrect on all accounts and especially wrong when the counter-factual methods of anti-piracy enforcement measures, and malware effects of using pirate sites are taken into account.

Geist asserts that the proposal will negatively impact privacy is the claim (addressed below) site blocking of pirate sites will lead to blocking of VPNs used to access U.S. Netflix. There is no

more than two thousand works that are the subject of this case in the face of their massive violation since, generally speaking, said measure will prevent Internet users in Spain from having normal access to the content offered illicitly on the website of the piratebay group.”

¹⁹⁰ *Warner Bros. Entertainment Norge AS v. Telenor Norge AS et al.*, 15-067093TVI-OTIR/05, Norway Oslo District Court (1 September 2015) “The consideration of the ISPs does not support not issuing an order. They are in such situations as neutral intermediaries best placed to stop the infringements by blocking their customers' access to notoriously infringing websites. Orders against the ISPs are an appropriate and proportionate measure in this matter, even if it will entail costs and disadvantages. Such orders do not interfere with the core activity of the ISPs. The suggested blocking method in this matter is further already being performed by the ISPs with respect to undesirable content such as spam and child pornography... The court also finds that the disadvantages and the costs that the ISPs incur with an order to block The Pirate Bay do not seem disproportionate or costly.”

¹⁹¹ *Associação Para a Gestão e Distribuição de Direitos et al. v. Acessos e Redes de Telecomunicações et al.*, Portugal Tribunal of Intellectual Property (24 February 2015) “However, it soon turns out that, despite having been stated, it was not demonstrated that implementing such DNS blocking measures entails significant costs or resource allocations, but only the simple human resources to carry out the necessary technical action; we do not think that this is a sacrifice for the defendants, much less that such a need has relevance for its operation, because they also have to comply with numerous other rules and legal and administrative constraints that imply costs and much more significant resources, i.e. these are actions that fit perfectly in the normal legal obligations of operators and that will always have to be part of their business.”

¹⁹² *Sony Music Entertainment Sweden et al. v. B2 Bredband AB*, PMT 11706-15, Sweden, Patent and Market Appeals Court (13 February 2017) “An additional condition to issue an injunction subject to a penalty of a fine is that such a measure is proportionate. When assessing the proportionality, the court must strike a balance between the fundamental rights upheld by the legal regime... The requested injunction subject to a penalty of a fine would admittedly limit B2 Bredband's abilities to conduct its business, i.e. the company's freedom of enterprise. The company would be forced to take administrative and technical measures that would entail extra costs for the company. However, as remarked by the CJEU in its judgment in the UPC Telekabel case, such an injunction would not affect the very substance of the freedom of enterprise of an Internet service provider (see para 51 of the judgment). B2 Bredband's parent company after decisions rendered by courts in other countries, already blocks subscribers' access to certain domain names and web addresses. B2 Bredband has also informed that the requested measures as such entail costs but that the costs are in a range that the company would be able to handle as part of its normal operations. The Patent and Market Appeals Court therefore holds that an injunction is proportionate also with regard to the restriction of the freedom of enterprise that the injunction would entail.”

basis to assume this to be the case and it would certainly require another application to the Commission for a situation that is not at all comparable to the FairPlay proposal.

He also asserts that “the identification of piracy sites and usage by subscribers depends in part upon snooping into Internet users’ online activities”. Geist claims that ISPs will “have incentives to track user activity by inspecting unencrypted communications to identify which sites are being visited.”

Far from increasing any privacy risks for Canadians, the proposal does the opposite. To establish that a site is a piracy site there is no need to collect any personal information of Canadians. What is being targeted is the piracy site, not the infringing actions of individuals. While the evidentiary requirements will depend on the criteria that are established in public consultations for the IPRA to use, the most likely kind of evidence that would be needed to prove use of a piracy site would be Alexa (or like) traffic data. There should be no need to prove that any specific Canadian used a site; only that many computers with IP addresses from Canada (which the copyright holders would not know) visited the piracy site.

However, even if there was a need for copyright holders to monitor the use of piracy sites, the only information that would be collected would be IP address (and perhaps port) information. This is information that Canada not only allowed but specifically encouraged to be collected through its adoption of the notice-and-notice system, something that Geist strongly advocated for throughout the copyright reform process. The IP addresses would only have to be used to lookup whether the users were from Canada using one of the many IP address lookup services available on the web. No actual subscriber information would be required. However, even if it did involve collecting such information it would not violate privacy rights of Canadians because of exemptions under Canada’s federal privacy law, PIPEDA.¹⁹³

Moreover, even where personal subscriber information has been asked for in the context of Norwich orders, the policy of the courts has been to order disclosure. Sexton J.A. of the Federal Court of Appeal in the *BMG Canada Inc. v. Doe* case expressed the reasons as follows.¹⁹⁴

¹⁹³ See s7(1)(b) and 7(1)(d) of PIPEDA which permits collection and use of personal information for the purposes of investigating a contravention of the laws of Canada.

¹⁹⁴ *BMG Canada Inc. v. Doe*, 2005 FCA 193 (C.A.).

Intellectual property laws originated in order to protect the promulgation of ideas. Copyright law provides incentives for innovators---artists, musicians, inventors, writers, performers and marketers---to create. It is designed to ensure that ideas are expressed and developed instead of remaining dormant. Individuals need to be encouraged to develop their own talents and personal expression of artistic ideas, including music. If they are robbed of the fruits of their efforts, their incentive to express their ideas in tangible form is diminished.

Modern technology such as the Internet has provided extraordinary benefits for society, which include faster and more efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.

In *Voltage Pictures LLC v. John Doe*¹⁹⁵ the Federal Court addressed the position ISPs should take in Canada when faced with a motion to disclose subscriber information in an infringement case. The court stated that normally, ISPs should facilitate the legitimate efforts of rights holders obtain subscriber information:

. . .it appears that Voltage has a strong prima facie case establishing piracy of its copyright product by the fact that TekSavvy's subscribers are downloading its materials without any possible suggested colour of right. Piracy of copyrighted materials on the Internet is a serious issue in North America. The Court's general policy therefore, should be to support measures that reasonably deter such illegal conduct, in which category I place Voltage's litigation, as it appears to be brought on a bona fide basis to deter such activity.

. . .the policy in these types of motions should normally be to facilitate the plaintiff's legitimate efforts to obtain the information from ISPs on the prima facie illegal activities of its subscribers.

An Irish case also considered whether the collection of IP address information in the course of anti-piracy investigations violated data protection legislation. The court concluded that individuals involved in peer-to-peer file sharing do not have a reasonable expectation of privacy and that their interests are far outweighed by those of the copyright owners who are being damaged by online infringements.

An activity of swarm participation for peer-to-peer downloading does not legitimately carry the expectation of privacy. It is flying in the face of common sense for the Data Protection Commissioner to equate participation in an open communication with all comers on the internet for the purpose of illegal downloading of copyright material with interception, with tapping or with listening. Those concepts are rightly to be deprecated as illegal in circumstances of privacy. That is not the situation here: there is no

¹⁹⁵ *Voltage Pictures LLC v. John Doe*, 2015 FC 1364.

legitimate reposing of trust pursuant to contract or reasonable expectation that when a person goes on the internet with a view to uploading or downloading what does not belong to them. That circumstance does not give rise to any constitutional entitlement or human right to remain immune from a music company also participating in that open forum to discover the economic damage that is being done to it and to creative artists. The interest of music companies is proper and proportionate. It is beyond doubt that while each individual act of copying, in itself, does little damage the reproduction of that activity by millions repeated over time is industrial in scale. The response of internet service providers of doing nothing perhaps reflects the greater economic strength of intermediaries as compared to creative people or recording companies. There is also the immeasurable and disproportionate power of these peer-to-peer swarms which are increasingly rendering the entitlement to those on whom creativity depends to no consideration...

The law does not, however, set intellectual property rights at naught because of the involvement of the internet.¹⁹⁶

Courts in the United States have also held that individuals engaged in peer-to-peer file sharing do not have any reasonable expectations of privacy.¹⁹⁷ As one U.S. court put it "[I]f an individual subscriber opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."¹⁹⁸

Geist also claims that the process of blocking sites may also raise privacy concerns. He indicates this is more likely to be a problem if deep packet inspection is used, but properly notes that the specific method of blocking is not yet known. He also doesn't indicate how likely use of deep packet inspection would be, especially given that, internationally, site blocking for copyright purposes has relied mainly on IP address, DNS, URL or a hybrid of such methods. In any event, the method of blocking the IPRA would recommend would be something that could be part of its consultation.

What is also important in considering Geist's arguments is the counter-factual, namely would the proposal increase or decrease the privacy of Canadians compared to other remedies that are available? When so considered the proposal is much better and at worst, no worse than the alternatives.

¹⁹⁶ *EMI Records (Ireland) Ltd & Others –v- Data Protection Commissioner*, [2012] IEHC 264, High Court of Ireland (27 June 2012),

¹⁹⁷ *Sony Music Entertainment Inc. v. Does*, 1-40 326 F. supp. 23 556 (S.D.N.Y. 2004), *Interscope Records v. Duty*, 79 U.S.P.Q.2d 1043 (D.Ariz.2006)

¹⁹⁸ *Recording Industry Association of America, Inc. v. Verizon Internet Servs., Inc.*, 351 F. 3d 1229 (D.C. Cir.2003); Quoted in *Sony Music Entertainment Inc. v. Does*, 1-40 326 F.Supp. 23 556 (S.D.N.Y. 2004)

Personal actions against Canadians who use piracy sites requires the monitoring of individuals' use of piracy sites, including monitoring what is downloaded or offered for uploading. To pursue such actions rightsholders have to obtain, through Norwich orders, subscriber information, something the proposal does not require.

Geist suggests that prior to proceeding with the proposal, the coalition members should have gone to court to obtain blocking orders using the *Equustek* case as a precedent. Even if one were to assume that this kind of proceeding does not require an underlying claim for infringement against individuals, it would at the very least require the collection of the same type of information as would be required in a proceeding brought before the CRTC. Further, ISPs would also have to implement the blocking order which would not reduce in any way the potential, such as there may or may not be, to the use of personal information of Canadians.

Moreover, Geist fails to take into account the privacy violations experienced by Canadians in using these pirate sites. Many pirate sites contain or distribute malware that can expose users to identity theft, financial loss, and hackers taking control of their computers.¹⁹⁹ In a recent study of the issue, the Technology Policy Institute concluded that using pirated materials increases a user's risk of being infected with malware. According to the authors:²⁰⁰

For years, those of us who study the effects of piracy have focused on two main questions. First, does it hurt creators, by reducing demand for what they produce? Here the answer is clearly yes: the vast majority of peer-reviewed studies have found that piracy hurts demand and overall firm profitability, and that anti-piracy measures can cause some consumers to return to legal channels. Second, does piracy benefit consumers, by providing them access to products they wouldn't have paid to consume? This question is asked less frequently than the first, but the growing consensus answer seems to be no: several recent studies (for example, here and here) suggest that piracy can hurt consumers by reducing the incentives for producers to invest in and create new products.

However, while these questions have been studied widely, there's another one worth asking: Does piracy also hurt consumers by exposing them to malware and other malicious software?

The problem is real. For users to access and download pirated content, someone has to make it available, and most of the sites that make pirated content available are in it for

¹⁹⁹ Amy Kraft "A third of pirated movie sites spread malicious software, report says" CBS NEWS December 14, 2015, <https://www.cbsnews.com/news/pirated-movie-video-download-sites-spread-malicious-malware/>.

²⁰⁰ Michael D. Smith and Rahul Telang , Piracy and Malware: There's No Free Lunch | The Technology Policy Institute, March 13, 2018, <https://techpolicyinstitute.org/2018/03/13/piracy-and-malware-theres-no-free-lunch/>.

the money. The people who run these sites typically make money by displaying advertisements—and, in some cases, by hosting or linking to content that contains malware. Designed to gather data from users' computers, or even to control them, malware can be very profitable, and as a result it's a danger that users of pirated material regularly have to contend with.

But does using pirated materials increase a user's risk of being infected with malware?...

To answer these questions, we conducted a study on a unique dataset of close to 250 users who form part of an IRB-approved panel within CMU's Security Behavior Observatory project....

The results were clear. The more our users visited piracy sites, we found, the more often their machines got infected with malware...

Piracy, once again, turns out not to offer the free lunch that it appears to.

Geist claim: slippery slope; it will inevitably result in blocking for other IP purposes

Geist claims that the proposal will inevitably result in blocking sites other than those targeted by the proposal. For example, he says "it would not be surprising to find legitimate services streaming unlicensed content as the next target." He uses U.S. Netflix as an example as a site that might be targeted.²⁰¹ Another is the use of virtual private networks (VPNs) that allow users to access out-of-market content such as U.S. Netflix. It is hard to characterize this claim as anything other than unsubstantiated conjecture. The proposal calls for blocking of only "websites and services that are blatantly, overwhelmingly, or structurally engaged in piracy."

The coalition recommended that the Commission establish criteria against which both it and the IPRA could evaluate whether a particular site is blatantly, overwhelmingly, or structurally engaged in piracy. The proposal provides examples of criteria that could be used in connection with determining whether a location on the Internet is blatantly, overwhelmingly, or structurally engaged in piracy: (a) The extent, impact, and flagrancy of the website's piracy activities; (b) The disregard for copyright demonstrated by the website's owners, pirate operators, or users; (c) Whether the website is expressly or implicitly marketed or promoted in connection with potential infringing uses; (d) The significance of any non-infringing uses, compared to the infringing uses; (e) The effectiveness of any measures taken by the website to prevent infringements; (f) Any other relevant finding against the website, related websites, or the website's owners in Canada or any other jurisdiction by a court or administrative tribunal; and (g) Any efforts by the website's owners or members to evade legal action.

²⁰¹ He repeats this when claiming that the proposal would increase privacy risks.

There is no good reason to believe that the 25 member coalition intends to target sites other than the type they propose, or to believe that even if they did, that the CRTC would agree to such a changed mandate.

Geist claim: more slippery slopes; the proposal will lead to blocking for other purposes

Geist warns that if the Commission was to order blocking for copyright, this would inevitably expand to block for other illegal content such as hate speech, online gambling and other regulated activities.

There is no reason to be concerned about targeted blocking to deal with sites that are clearly devoted to dissemination of other illegal content. Other liberal democratic countries including members of the European Union already engage in website blocking to protect members of the public from illegal activities such as from malware, investment fraud, hate speech, child abuse materials including child pornography, prostitution, speech inciting violence, online gambling, prohibiting dissemination of Nazi war memorabilia, and terrorism related content, trade-mark infringement, and copyright infringement, all without breaking the Internet.²⁰²

The use of website blocking as a tool to protect the public from illegal materials needs to be assessed with the emerging and important recognition that, for all its good, the Internet is increasingly used for all manner of crimes and to spread false information (fake news), and racist and hateful materials.²⁰³ There is also an increasing realization that what is illegal offline should also be illegal online,²⁰⁴ and that Internet intermediaries, from ISPs, search engines, to

²⁰² Jaan Riordan, *The Liability of Internet Intermediaries* (Oxford University Press, 2016), Chapters 14 and 15; Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'", ITIF, August 2016, <http://www2.itif.org/2016-website-blocking.pdf>.

²⁰³ See, "France's government to fight racism and anti-Semitism online", The Washington Post, March 19, 2018, https://www.washingtonpost.com/world/europe/frances-government-to-fight-racism-and-anti-semitism-online/2018/03/19/8098c21e-2b5a-11e8-8dc9-3b51e028b845_story.html

²⁰⁴ See, European Commission "A Europe That Protects" Countering Illegal Content Online", http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50096 "The Juncker Commission made security a top priority from day one. It is the most basic and universal of rights to feel safe in your own home or when walking down the street. Europeans rightly expect their Union to provide that security for them – online and offline. The Commission has taken a number of actions to protect Europeans online – be it from terrorist content, illegal hate speech or fake news. We are working closely with the Internet companies, Member States and EU Agencies through various initiatives and we are continuously looking into ways we can improve our fight against illegal content online." "Illegal content means any information which is not in compliance with Union law or the law of a Member State, such as content inciting people to terrorism, racist or xenophobic, illegal hate speech, child sexual exploitation, illegal commercial practices, breaches of intellectual property rights and product safety. What is illegal offline is also illegal online." Also, "Elections Canada prepares to fight fake

social network platforms, must act responsibly and play a role in countering these threats. Recently, and even before the Facebook/Cambridge Analytica fiasco,²⁰⁵ there has been a “sea change” on digital governance issues²⁰⁶, with even the “inventors” of the Internet Sir Tim Berners-Lee²⁰⁷ and Vint Cerf²⁰⁸ calling attention to the problems.

news, foreign influence in 2019 vote”, CBC News, <http://www.cbc.ca/news/politics/elections-canada-fake-news-voting-1.4582291?cmp=rss>

²⁰⁵ Canada's privacy watchdog launches investigation into Facebook after allegations of data leak – Politics, March 20, 2018, <http://www.cbc.ca/news/politics/canada-privacy-watchdog-facebook-investigation-1.4585210?cmp=rss>

²⁰⁶ Alex Boutilier :”Internet giants should support local news, culture, Melanie Joly says”, Toronto Star, March 14, 2018, <https://www.thestar.com/news/canada/2018/03/14/internet-giants-should-support-local-news-culture-melanie-joly-says.html> “But in recent weeks, the Liberals have taken a more aggressive tone with digital disrupters — saying the companies need to address problems like the spread of disinformation online, or face tighter federal regulations. Taylor Owen, a digital media and global affairs researcher at the University of British Columbia, said he feels there’s been a “sea change” within the Canadian government on digital governance issues.” Hugh Stephens “Internet Platforms: It’s Time to Step up and Accept Your Responsibility (Or Be Held Accountable)”, March 25, 2018, <https://hughstephensblog.net/2018/03/26/internet-platforms-its-time-to-step-up-and-accept-your-responsibility-or-be-held-accountable/>, “The tide is turning, and the behaviour and role of the big Internet platforms is starting to lead to important questions being asked. If the platforms continue to act as if they were a law unto themselves, what is the appropriate role for regulation and legislation? To the Internet platforms I say, start assuming responsibility for your actions or accept the consequences.”

²⁰⁷ Sir Tim Berners-Lee “The web is under threat. Join us and fight for it. – World Wide Web Foundation”, <https://webfoundation.org/2018/03/web-birthday-29/> “The threats to the web today are real and many, including those that I described in my last letter — from misinformation and questionable political advertising to a loss of control over our personal data...

What’s more, the fact that power is concentrated among so few companies has made it possible to weaponise the web at scale. In recent years, we’ve seen conspiracy theories trend on social media platforms, fake Twitter and Facebook accounts stoke social tensions, external actors interfere in elections, and criminals steal troves of personal data.

We’ve looked to the platforms themselves for answers. Companies are aware of the problems and are making efforts to fix them — with each change they make affecting millions of people. The responsibility — and sometimes burden — of making these decisions falls on companies that have been built to maximise profit more than to maximise social good. A legal or regulatory framework that accounts for social objectives may help ease those tensions.”

²⁰⁸ See, the article by “the father of the Internet” Vinton Cerf writing about the problem with fake news, Vinton Cerf, “Vint Cerf: In 2018, we will tackle the Internet’s dark side” Wired, Jan 6, 2018, <http://www.wired.co.uk/article/vint-cerf-internet-free-speech-censorship-fake-news>. “The empowerment of individuals has been nothing short of exhilarating - but now we are starting to see the consequences. Freedom to speak has never been more available, but in the resulting babel, truth is obscured by manufactured falsehoods, misrepresentations, fake news, alternative facts and a medley of other phenomena. In 2018 we will see a significant reaction to these side-effects and will grasp the nettle of how to balance free speech with an open Internet...

So here is the conundrum for our increasingly connected world: how do we stay aware of what is going on in the world and in the minds of its citizens while seeking to limit the pernicious consequences of unbridled freedom to spew hatred, falsehoods and society-damaging ideologies? How do we instil a capacity for critical thinking in our citizens so they can winnow wheat from chaff? Is critical thinking sufficient defence against the digital acid rain that threatens

Recently, the U.S. House of Representatives passed an anti-sex trafficking bill that could make websites liable for enabling sex traffickers, after the technology industry refused to implement voluntary measures. The bill represents the growing techlash against large U.S. technology companies arising from their expansive power over people's lives and the intense scrutiny over their role in Russian election meddling, the spread of online conspiracy theories, and addiction to social media.²⁰⁹

The European Commission earlier this month recommended a set of operational measures while it considers further legally binding regulatory measures for voluntary monitoring and takedowns (without court orders) of all forms of illegal content ranging from terrorist content, incitement to hatred and violence, child sexual abuse material, counterfeit products and copyright infringement. These measures are not premised on the use of court orders because of the need to act quickly to deal with harms caused by illegal content.²¹⁰ In fact, member states

to poison the ocean of useful online information? These are the questions that should be at the front of our minds in 2018.”

See, also Laura Sydell, “The Father Of The Internet Sees His Invention Reflected Back Through A ‘Black Mirror’” all tech considered, Feb. 20, 2018, <https://www.npr.org/sections/alltechconsidered/2018/02/20/583682937/the-father-of-the-internet-sees-his-invention-reflected-back-through-a-black-mir>, “We know how that turned out. People with less lofty ambitions than Cerf used that loophole for cybercrime, international espionage and online harassment.” Cerf admits all that dark stuff never crossed his mind. “And we have to cope with that — I mean, welcome to the real world,” he says.”

²⁰⁹ Steve Overly et al, “House passes anti-sex trafficking bill in defeat for tech industry”, https://www.politico.com/story/2018/02/27/house-passes-anti-sex-trafficking-bill-367692?utm_content=buffer461&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

²¹⁰ “A Europe that protects: Commission reinforces EU response to illegal content online”, Brussels, 1 March 2018, http://europa.eu/rapid/press-release_IP-18-1169_en.htm. The Press Release announcing the initiative provided some of the rationale as follows:

“Vice-President for the Digital Single Market Andrus Ansip said: “Online platforms are becoming people's main gateway to information, so they have a responsibility to provide a secure environment for their users. What is illegal offline is also illegal online. While several platforms have been removing more illegal content than ever before – showing that self-regulation can work – we still need to react faster against terrorist propaganda and other illegal content which is a serious threat to our citizens' security, safety and fundamental rights.”

The spread of illegal content online undermines the trust of citizens in the Internet and poses security threats. While progress has been made in protecting Europeans online, platforms need to redouble their efforts to take illegal content off the web more quickly and efficiently. Voluntary industry measures encouraged by the Commission through the EU Internet Forum on terrorist content online, the Code of Conduct on Countering Illegal Hate Speech Online and the Memorandum of Understanding on the Sale of Counterfeit Goods have achieved results. There is however significant scope for more effective action, particularly on the most urgent issue of terrorist content, which presents serious security risks.”

in the EU permit blocking of content without court order to prevent access to content of substantial public concern.²¹¹

The Canadian Office of the Privacy Commissioner (OPC) also recently recommended in the Draft OPC Position on Online Reputation,²¹² that search engines be required in appropriate circumstances to de-index online locations that make available personal information about individuals in order to protect their reputations. The OPC recommended that this should be done without the need for court orders and that if there was ultimate access to an independent arbiter in contested cases, search engines should provide the first level of review of a de-indexing request. Doing so would arguably promote, rather than hinder, access to justice and the rule of law by providing a practical and expedient remedy for individuals. According to the OPC:

In submissions, it was suggested that it is inappropriate for a private sector organization to make decisions balancing privacy rights against the right to expression...

“Today’s Recommendation sets out operational measures to ensure faster detection and removal of illegal content online, to reinforce the cooperation between companies, trusted flaggers and law enforcement authorities, and to increase transparency and safeguards for citizens:

Clearer ‘notice and action’ procedures: Companies should set out easy and transparent rules for notifying illegal content, including fast-track procedures for ‘trusted flaggers’. To avoid the unintended removal of content which is not illegal, content providers should be informed about such decisions and have the opportunity to contest them.

More efficient tools and proactive technologies: Companies should set out clear notification systems for users. They should have proactive tools to detect and remove illegal content, in particular for terrorism content and for content which does not need contextualisation to be deemed illegal, such as child sexual abuse material or counterfeited goods.

Stronger safeguards to ensure fundamental rights: To ensure that decisions to remove content are accurate and well-founded, especially when automated tools are used, companies should put in place effective and appropriate safeguards, including human oversight and verification, in full respect of fundamental rights, freedom of expression and data protection rules....”

²¹¹ See, Council Of Europe, “Comparative Study on blocking, filtering and take-down of illegal internet content (2015)”, <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>

“In relation to child abuse material, terrorism, criminality (in particular hate crimes) and national security, many of the states with targeted legal rules for the removal of internet content provide for the urgent blocking of such material without the need for a court order. Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves. In other countries, such as Finland, where a court order is otherwise needed, hosting providers who have knowledge of such material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.”

²¹² Jan 26, 2018, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/?platform=hootsuite.

While this is a legitimate concern we also note that organizations do regularly engage in such balancing to some extent – for instance, in establishing terms of service which may result in content, statements or even entire accounts being removed. Search engines, in particular, already have in place mechanisms to consider de-indexing requests and remove content which is potentially harmful (e.g. credit card numbers; images of signatures) or illegal (e.g. copyright infringement) from their search results...

Some have suggested that de-indexing requests should only be considered by an oversight body or a court given the fundamental rights at stake. While individuals and search engines should ultimately have access to review by an independent arbiter in contested cases, we consider it appropriate to have search engines providing the first level of review of a de-indexing request. Indeed, having search engines initially assess de-indexing requests arguably promotes, rather than hinders, access to justice and the rule of law by providing a practical and expedient remedy for individuals.

The OPC also recommended that individuals should have a right of “erasure” and that web sites should voluntarily engage in source amendment/takedowns in appropriate circumstances. A Parliamentary Committee reviewing Canada’s privacy legislation, PIPEDA, also recently recommended that Parliament consider amending PIPEDA to provide an express right of erasure and “right to be forgotten”. Although the exact mechanisms to be used were not part of the proposals, the recommendations did not suggest that this had to be accomplished through court orders.²¹³

The solutions to online illegal content and whether website blocking is appropriate in any given case, must as a matter of pragmatic reality, be based on an assessment of multiple factors.

We should not fear the use of an appropriate and targeted measure to counter illegal activity because it could also be used to counter other illegal activity. If anything, recent events teach us that we must ensure responsibility and accountability in online activities and be prepared to take measures needed to protect the public.

Geist himself is a proponent of and has defended website blocking of foreign websites to address online child pornography.²¹⁴ His rationale for distinguishing between that and blocking for copyright purposes, both before and after the FairPlay proposal, relies on the extent to which he views the dissemination of child pornography to be problematic (versus copyright infringement) and because he says:

²¹³ Standing Committee on Access to Information, Privacy and Ethics “Towards Privacy by Design: A Review of Personal Information Protection and Electronic Documents Act”, <http://ow.ly/7VH330iHAuk>

²¹⁴ Michael Geist, Child Pornography Blocking Plan a Risk Worth Taking, Dec. 4, 2016, <http://www.michaelgeist.ca/2006/12/project-cleanfeed-column/>.

the blocking of child pornography can be justified on the grounds that even accessing child pornography is a criminal offence. Not so for viewing a streaming video, whether authorized or unauthorized.

I agree with Geist that child pornography should be blocked. Geist is wrong, however, that merely accessing child pornography is a criminal offense. Under Section 163.1 of the *Criminal Code* it is an offense to access child pornography only where the person knowingly causes child pornography to be viewed by, or transmitted to, himself or herself. Further, there is an express exception where a person has “a legitimate purpose related to the administration of justice or to science, medicine, education or art; and does not pose an undue risk of harm to persons under the age of eighteen years”.

Geist is also wrong to suggest that merely accessing infringing copying content cannot be illegal. For example, in the *ITVBox.net* case the Federal Court of Canada expressed the opinion that individuals that operate equipment to receive a programming signal that have been decoded in contravention of the *Radio-Communication Act* violate that Act.²¹⁵ Doing so could be an offense under sections 9(1)(d) and 10(1)(b) of the Act. Further, courts in the UK have found that persons that receive infringing copies of copyright content using an online file sharing site like The Pirate Bay can be jointly liable for the infringements.²¹⁶

Geist’s attempt to justify website blocking only where based on mere access of content being illegal cannot be accepted as a justifiable basis for excluding the availability of blocking in other circumstances. If it did, then according to Geist’s indefensible distinction, it would be wrong to block child porn websites in Canada, even though it is internationally accepted that this should be done and can be defended on multiple grounds.

Decisions as to whether there should be blocking orders related to other illegal conduct have to be assessed on a case by case basis. In my view, it is wrong to regard an expansion of website blocking to content other than copyright materials as *prima facie* bad policy. Like child pornography, each situation must balance the proposed benefits and harms.

²¹⁵ *Bell Canada v ITVBOX.NET*, 2016 FC 612 “I also find that the Plaintiffs have made a strong prima facie case that the devices sold by the Defendants are used to access content that may contravene paragraph 9(1)(c) of the Radiocommunication Act. Streaming sites that rebroadcast the Distribution Plaintiffs’ programming are not authorized to communicate those works to the public. A user who accesses these works might also contravene the *Radiocommunication Act*.”

²¹⁶ *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors*, [2012] EWHC 268 (Ch) (20 February 2012).

Geist claim: more slippery slopes, the proposal will turn the CRTC into a content regulatory authority

Geist tries to assimilate blocking illegal pirate sites to content regulation. That is no more true than arguing that when courts grant injunctions prohibiting the dissemination of materials that are defamatory, in violation of child pornography or pornography laws, infringe copyrights, or are otherwise illegal -which courts do all the time – they are engaging in “content regulation”.

He cites a paragraph from the CRTC website that says “In Canada, services that broadcast over the Internet don’t need a licence from the CRTC, as we exempted them from this obligation. We do not intervene on content on the Internet.” He says this “reflects how the CRTC sees itself and how it wants to be seen, that it does not licence or judge Internet content nor is it empowered by legislation to do so.”

The statement that the CRTC does not intervene on content on the Internet was simply based on the fact that the CRTC issued an exemption order under the *Broadcasting Act* for Internet services. That order was issued in 1999 and updated in 2012. But this does not mean the CRTC does not have the jurisdiction to rescind the exemption order, or to impose terms and conditions that relate to content on Internet services covered by that order. In its 1999 policy, the CRTC clearly indicated that most Internet video services would fall under its regulatory jurisdiction, absent an exemption. And subsection 9(4) of the *Broadcasting Act* specifically allows the CRTC to exempt persons from the requirements of the Act “on such terms and conditions as it deems appropriate.”

Geist also states that “the attempt to incorporate the *Broadcasting Act* into the argument runs counter to the Supreme Court of Canada’s 2012 ISP Reference, which leaves no doubt that ISPs simply do not fall under that Act when transmitting content”.

The Supreme Court did rule that ISPs could not be directly regulated under the *Broadcasting Act* in their conduit of information capacities for content broadcast by others. But the jurisdiction to issue blocking orders being relied on in the proposal derives from the *Telecommunications Act*, not the *Broadcasting Act*. And there is nothing in the judgment of the Supreme Court that precludes CRTC regulation of Internet program services under the *Telecommunications Act* or even under the *Broadcasting Act* if and when ISPs are broadcasting to Canadians.

Geist claim: Canada has robust laws and doesn't need more legal tools to target offshore pirate sites

Geist claims Canada “has some of the world’s toughest anti-piracy provisions” and doesn’t need any new laws to target online piracy. Although Geist makes references to copyright laws that exist in Canada, he makes no attempt to show whether or how they could be useful in combatting the threats the FairPlay proposal is designed to counter. Many of his claims would be misleading to the average person who would not understand the lack of connection between an existing cause of action and one that had some relevance to countering online piracy.

Geist points to our anti-circumvention laws that target mod-chip sellers as an example of our tough anti-piracy laws. However, it is misleading to suggest that this law has any applicability to combating online streaming piracy sites. Although our TPM laws have been found to be adequate against sellers of mod-chips for video gaming devices, these laws provide no remedies against pirate online streaming, peer-to-peer file sharing, or download services.

He also points to Canada’s secondary infringement enablement provision. Here again, he fails to even argue how this cause of action would be effective against foreign pirate streaming sites. It is quite conceivable that under the real and substantial connection test a court would find that the cause of action would apply to foreign services that primarily enable copyright infringement and that target Canadians with illegal streaming services.²¹⁷ However, the operators of pirate streaming websites often hide their identities such as through domain privacy protection services and obtain hosting and other services from jurisdictions that are not friendly to rights holders.²¹⁸ Direct enforceable remedies to make them cease their activities is frequently impossible. For example, The Pirate Bay has been blocked by around the world and its originators were jailed by a Swedish court.²¹⁹ Yet, it still continues to defy and evade legal measures to shut it down.²²⁰ It is misleading to suggest that enablement is also an effective remedy against foreign online piracy sites.

²¹⁷ *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45.

²¹⁸ Jo Oliver and Elena Blobel, “Website Blocking injunctions – A Decade of Development”, in Jacques de Werra (Ed) et al., *Droit d’auteur 4.0*, Schulthess Verlag (2018) (“*Oliver Website Blocking injunctions*”).

²¹⁹ *Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v Sweden* - 19 February 2013) (ECHR Case 40397/12).

²²⁰ *Stichting BREIN v Ziggo BV*, THE HAGUE COURT, Commercial Law Division, Case/Docket Number District Court C/09/535341/KG ZA 17-891, Sept 22, 2017 “In the view of the District Court the subsidiarity condition has been met. Brein and other collective rights bodies already held several proceedings against The Pirate Bay and its operators and furthermore against hosting providers of

Geist also relies on Canada's statutory damages regime. However, here again he fails to show that this regime, which was substantially weakened by the 2012 copyright amendments, could pragmatically be enforced against a foreign online pirate site or that such sites would have the assets necessary to pay any damages awarded against them. This claim is also misleading.

Geist points to the *ITVbox.net* interlocutory injunction²²¹ against Kodi and other ISD distributors. He also refers to the Anton Piller order and interlocutory injunction in the *TVAddons.net* case against website operator Adam Lackman that made available software add-ons specifically adapted to enable users with ISDs to access illicit streaming sites.²²² He argues the decisions demonstrate there is no need for the proposed blocking regime.²²³ He is wrong.

It is true that the Federal Court of Canada has on interlocutory motions granted injunctions against Canadian sellers of ISDs and a Canadian website operator who made add-ons available. In this regard, Canadian law has, so far, kept pace with those of our international peers where similar remedies have been granted.²²⁴

The Pirate Bay. However, The Pirate Bay is still online because (the operators of) The Pirate Bay disregards the court decisions. Thus the users of The Pirate Bay, including part of the subscribers of Ziggo and XS4ALL can continue their infringing acts."

²²¹ *Bell Canada v. 1326030 Ontario Inc. (iTVBox.net)*, 2016 FC 612, aff'd 2017 FCA 55.

²²² *Bell Canada v Adam Lackman dba TVADDONS.AG*, 2018 FCA 42.

²²³ "University of Ottawa internet law professor told MobileSyrup via email "that the [Lackman] decision highlights yet again how Canada already has some of the toughest anti-piracy laws in the world and why the proposed site blocking system is so ill-advised." Sameer Chhabra, "Bell, Rogers, Videotron granted appeal against Kodi add-ons distributor", Mobilesyrup. Feb. 21, 2018, <https://mobilesyrup.com/2018/02/21/bell-rogers-videotron-appeal-kodi-media-player-add-ons-distributor/>. Also, Geist tweet, "Whatever your thoughts on TVAddons, this case again confirms that Canada has some of the toughest anti-piracy laws in the world and - as @NavdeepSBains noted - that there are already many legal tools available to copyright owners" 2018-02-21, 4:05 PM"

²²⁴ For example, in *Brein v Wullems' Case C-527/15 ECLI:EU:C:2017:300* the Court of Justice of the European Union found that the sale of the filmpeleer multimedia player ISD infringed the exclusive copyright making available right; U.S. courts have issued a preliminary injunctions prohibiting the distribution of ISDs and applications that were marketed, promoted, and adapted to receive infringing streams delivered from streaming servers and peer-to-peer networks. *China Cent. Television v. Create New Technology (HK) Ltd.* 2015 WL 3649187 (C.D. Calif. Jun 11, 2015); *Universal City Studios Productions LLLP v TickBox TV LLC* (C.D.Cal. Jan 30, 2018); the Dutch anti-piracy Group BREIN also obtained an injunction against a company that operated the website MovieStreamer that sold Kodi-based software which could be used to access infringing TV, movie and sports streams based on infringement of the making available right. See, "The Kodi Crackdown is Now Targeting Stream Providers Who Don't Host the Content Themselves", Gizmodo UK, available at <http://www.gizmodo.co.uk/2017/10/the-kodi-crackdolwn-is-now-targeting-stream-providers-who-dont-host-the-content-themselves/>.

However, cases against such Canadian operators are, while very important, at best a whac-a-mole remedy. They target local provider/enablers of infringements, but there are many other providers, and remedies against this low level of contributor provide no relief against the foreign pirate sites that are the source of the content being illegally consumed. Geist doesn't try to argue the contrary.

Laws that provide relief only against individuals that sell ISDs and who make available add-ons if they happen to be located in Canada would be as productive as anti-drug laws that only target street corner and small time drug pushers and which provide no legal means of targeting the cartels, organized crime, or large scale drug syndicates or of seizing drug shipments at the border.

Genuine efforts to stem online piracy, like laws that attempt to address other illegal activities, require a mixture of complementary and appropriate measures including web site blocking. Website blocking has been recognized by courts as an effective way to combat internet piracy from foreign websites.²²⁵ That is why throughout the European Union, which also makes the sale of ISDs illegal,²²⁶ orders against ISPs are used to block the sources of illegal content. This includes injunctions against illegal streaming servers of soccer matches in the United Kingdom on behalf of the Premier League²²⁷ and on behalf of UEFA,²²⁸ the governing body of soccer in Europe.

Geist states that "Canadian law already provides for injunctive relief in appropriate circumstances with the Supreme Court of Canada's *Equustek* decision one of the more recent

²²⁵ See, *Société Française du Radiotéléphone et al. v. Orange et al.*, Case No: 14/03236, France, Paris Court of First Instance (04 December 2014) "the request to block access to the internet sites expressly referred to in the requests of the SCPP is the only genuinely effective manner that rightholders have at this time to fight against infringements of copyright on the internet."; *SCPP v. Orange S.A. et al.*, No. RG: 16/05527, France, Tribunal De Grande Instance De Paris (31 March 2016) "Consequently, the request to block access to websites specifically covered in the applications of the SCPP is the only way really effective currently available to rights holders intellectual property for the fight against piracy on the internet."

²²⁶ See *Filmpeler supra*.

²²⁷ *The Football Association Premier League Ltd v British Telecommunications Plc & Ors*, [2017] EWHC 480 (Ch) (13 March 2017). A subsequent injunction was granted in *Football Association Premier League Ltd v British Telecommunications plc*, [2017] EWHC 1877 (Ch).

²²⁸ *Union Des Associations Européennes De Football v British Telecommunications Plc & Ors*, [2017] EWHC 3414 (Ch) (21 December 2017). A blocking injunction has also been made by a court in Ireland, see, "Websites infringing TV and film copyright to be blocked", *The Irish Times*, January 15, 2018, <https://www.irishtimes.com/news/crime-and-law/courts/high-court/websites-infringing-tv-and-film-copyright-to-be-blocked-1.3356668>.

manifestations of courts issuing orders to non-parties in support of intellectual property rights” However, he acknowledges that there “is no guarantee that courts will issue such an injunction”. Yet, he says that rights holders ought to pursue this remedy before going the CRTC route.

Leaving aside the procedural challenges of obtaining a court order against all Canadian ISPs in a court proceeding, such litigation would be time consuming and expensive to pursue, especially with the attendant risk of appeals to the Supreme Court of Canada. Moreover, even if rights holders were to bring court proceedings for a blocking order and a court was disposed to make the order, rights holders could be met with Section 36 of the *Telecommunications Act* which has been interpreted by the CRTC as only conferring on it the power to make blocking orders against ISPs. Thus, given the current regulatory regime in Canada there are also cogent reasons for going directly to the CRTC in the first instance.

Geist has a history of opposing copyright laws to combat intellectual property violations. An assessment of the position he now takes on the state of Canadian laws should be assessed on the merits (canvassed above). It is also relevant, in this regard, to take into account his prior positions such as the following:

Geist opposed enacting the enablement cause of action to enable rights holders to shut down file sharing sites like isoHunt claiming our laws were adequate and that it would stifle innovation.²²⁹ Of course, he has since presented no evidence that they have stifled innovation.

Geist says in his FairPlay posts that the laws against ISDs used in the *ITVBox.net* decision can be used to fight online piracy, but when they were used in the *ITVBox.net* case he claimed that cracking down on them “Threatens to Chill Canadian Tech Innovation”.²³⁰ Again, despite making the claim more than two years ago he has presented no evidence that they have chilled innovation.

Before the *Equustek* decision was released he warned providing the remedy would turn the Internet into the wild west.²³¹ When the *Equustek* decision was released, he claimed it went too far.²³²

²²⁹ Barry Sookman, “Reining in the rhetoric on copyright reform”, Feb. 8 2012, <http://www.barrysookman.com/2012/02/08/reining-in-the-rhetoric-on-copyright-reform/>.

²³⁰ Barry Sookman “Why crackdown on pirate set-top boxes is good for innovation: a reply to Michael Geist”, Jan 29, 2016, <http://www.barrysookman.com/2016/06/29/why-crackdown-on-pirate-set-top-boxes-is-good-for-innovation-a-reply-to-michael-geist/>.

²³¹ Michael Geist, “How the Supreme Court can avoid turning the Web into a Wild West”, March 24, 2017, <https://www.theglobeandmail.com/report-on-business/rob-commentary/how-the-supreme-court-can-avoid-turning-the-web-into-a-wild-west/article33303774/>.

²³² Michael Geist, “Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results”, June. 28. 2017,

At the time Canada was considering entering into the TPP (with the US) it contained an article which required criminal sanctions against digital pirates who carry on businesses directed at content theft by removing rights management information (RMI) that identifies the owner of the copyright in a work. He called this “troubling” and opposed it.²³³

As has happened repeatedly in the past, Geist’s alarmist claims about the FairPlay proposal will turn out to have been unwarranted.

In 2015 Australia enacted a specific site blocking regime to address online piracy facilitated by foreign websites. The Explanatory Memorandum that accompanied the Bill which summarized the rationale for the enactment is apposite to the Canadian situation as well.²³⁴

Copyright protection provides an essential mechanism for ensuring the viability and success of creative industries by incentivising and rewarding creators. Online copyright infringement poses a significant threat to these incentives and rewards, due to the ease in which copyright material can be copied and shared through digital means without authorisation.

Where online copyright infringement occurs on a large scale, copyright owners need an efficient mechanism to disrupt the business models of online locations operated outside Australia that distribute infringing copyright material to Australian consumers. In addition, a consequence of fewer visitors at the particular online location may also impact the advertising revenue, which is often an integral element of the business models of these types of entities.

The Bill acknowledges the difficulties in taking direct enforcement action against entities operating outside Australia. The proposed amendments are intended to create a no-fault remedy against CSPs where they are in a position to address copyright infringement.

Why all this matters - Conclusion

The FairPlay proposal represents a well thought out approach to dealing with Internet piracy in the Canadian context. Yet, Geist has attempted to demonize it using, what appears to be, any contrived argument he can think of. He also has, as I showed above and in my prior blog post, tried to support his arguments with inaccurate and misleading information and arguments and by proffering references that don’t support his claims.

<http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results/>.

²³³ Barry Sookman “Grasping at straws: the trouble with ‘The Trouble with the TPP’, a further reply to Michael Geist”, April 17, 2016, <http://www.barrysookman.com/2016/04/17/grasping-at-straws-the-trouble-with-the-trouble-with-the-tpp-a-further-reply-to-michael-geist/>.

²³⁴ Australia Explanatory Memorandum to the *Copyright Amendment (Online Infringement) Bill 2015*, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r5446

Moreover, Geist postulates a radical net neutrality Internet Governance framework where courts and government agencies are powerless to intervene to halt illegal activities over the Internet. He goes further than even Mr LaRue, the former Special Rapporteur at the UN for freedom of expression that recognized that courts and government agencies have a right to make blocking orders. He takes a similarly unbalanced position in claiming that intervening to stop online theft is unnecessary by ignoring the well documented harms caused by illegal piracy sites,²³⁵ the evidence, including findings by courts that have studied this, that blocking orders are effective without any real risks of over-blocking, and without breaching fundamental freedom of speech rights.

What is even more troubling is that he engages in fear mongering. He tells average Canadians – who have no reason not to believe a Canada Research Chair - that the proposal is radical, breaks net neutrality rules, may violate their fundamental freedom of speech and privacy rights, will result in blocking access to U.S. Netflix, content blocking by the CRTC and will lead to who knows what else. We should expect much more from a Canada Research Chair in Internet and E-commerce Law.

Geist also knows that his blogs will be widely read and will be used by Internet activists and others to oppose the proposal and to provide similarly misleading information to the public to encourage them to oppose the proposal. Unfortunately, but quite predictably, his unfounded attacks are being relied upon by others to oppose the proposal using exaggerated and inflammatory arguments.²³⁶

²³⁵ See, M.D. Smith & R. Telang, Assessing The Academic Literature Regarding the Impact of Media Piracy on Sales (2012), accessed: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132153 (Study finding that peer reviewed journals spanning both music and motion picture sales, found evidence of statistically significant harm to sales of recently released content as a result of unauthorized file sharing.); “Piracy to cost TV and film industry US\$52bn by 2022”, Digital TV Europe, Oct 30, 2017, <http://www.digitaltveurope.com/2017/10/30/piracy-to-cost-tv-and-film-industry-us52bn-by-2022/>; “Pirates are selling cheap, live TV and some Canadians are signing up” CBC News March 30, 2018 <http://www.cbc.ca/beta/news/business/piracy-iptv-services-live-tv-1.4560320>. [The latest MUSO report for 2017, accessible at www.fairplaycanada.ca, ranks Canada at 11 in the world for TV piracy, with a total of 2.496 billion visits to piracy sites for 2017, with web streaming being the most popular form of unlawful content accessed.](http://www.fairplaycanada.ca)

²³⁶ See, for example, the Open Media campaign “Join the Day of Action against a Bell-led censorship initiative” Feb 22, 2018, available @ <http://rabble.ca/blogs/bloggers/open-medias-blog/2018/02/join-day-action-against-bell-led-censorship-initiative>. “This unprecedented Canadian proposal is deeply problematic for a number of reasons (as outlined by professor Michael Geist's series **The Case Against the Bell Coalition's Website Blocking Plan**), such as Canada already having some of the **toughest anti-piracy rules** in the world and the data showing **declining** piracy rates as well as

For example, OpenMedia has a “Don’t Censor Canada” website campaign encouraging Canadians to write interventions to the CRTC. It tells Canadians

“This dangerous and over-reaching proposal will lead to legitimate content and speech being censored, violating our right to free expression and the principles of Net Neutrality, which the federal government has consistently pledged support for.”

In its “Want to learn more?” section the first reference is to Geist’s blog posts stating “The Case Against the Bell Coalition’s Website Blocking Plan: Read this excellent series by University of Ottawa law professor Michael Geist”.²³⁷ The OpenMedia site contains a draft pre-written email to the CRTC which is premised on same inaccurate types of claims Geist has been advocating.²³⁸ OpenMedia also partnered with SumOfUs which has a pre-populated form e-mail which makes similar inaccurate claims about the proposal.²³⁹

a **booming television and streaming industry** -- contrary to the story Bell's coalition is telling the CRTC.”

Laura Tribe Executive Director, OpenMedia.”Bell's Website Blocking Plan Is Authoritarian Overkill”, http://www.huffingtonpost.ca/laura-tribe/internet-piracy-website-blocking-proposal-protest_a_23372670/?utm_hp_ref=ca-business. “Last month, experts, activists, policy-makers and citizens across the country were shocked by an unprecedented proposal to regulate the Internet that, if enacted, could change the way Canadians share and collaborate online forever.”.

²³⁷ <https://act.openmedia.org/dontcensor>. It also referred to an editorial in the Globe and Mail published before the proposal was even public that was heavily influenced by Geist’s misleading attacks on it. See, Barry Sookman “Globe and Mail editorial attacks on Canadian creators and broadcasters: what’s up with the Globe?” Jan 4, 2018, <http://www.barrysookman.com/2018/01/04/globe-and-mail-editorial-attacks-on-canadian-creators-and-broadcasters-whats-up-with-the-globe/>; also, Barry Sookman “Website blocking proposal good policy”, Dec. 8, 2018. <http://www.barrysookman.com/2017/12/08/website-blocking-proposal-good-policy/>. This is an instance of how his misleading writings influenced a mainstream media to uncritically repeat his views in an editorial and then how that editorial became a reference cited by OpenMedia to make its position appear credible. The Globe and Mail later published an op-ed of mine to help correct the misinformation from its editorial. Barry Sookman “Support for creators: pirate streaming and the value gap, my op-ed in the Globe” Jan. 19, 2018, <http://www.barrysookman.com/2018/01/19/support-for-creators-pirate-streaming-and-the-value-gap-my-op-ed-in-the-globe/>. Another op-ed of mine was published in The Hill Times, Barry Sookman “Why the CRTC should endorse FairPlay’s website-blocking plan: a reply to Michael Geist” Feb. 12, 2018, <http://www.barrysookman.com/2018/02/12/why-the-crtc-should-endorse-fairplays-website-blocking-plan-a-reply-to-michael-geist/>.

²³⁸ “I am gravely concerned about the recent proposal from the so-called “FairPlay Canada” coalition to introduce a mandatory website blocking system in Canada, administered by the CRTC. This proposal would result in sweeping Internet censorship, penalize everyday online activities, and threaten Canada’s Net Neutrality rules that keep the Internet a level playing field for all. This is simply unacceptable, and not the Canada that I want to live in.”

²³⁹ <https://actions.sumofus.org/a/send-an-email-to-protect-net-neutrality-now?source=campaigns> “I am deeply opposed to the recent proposal from the “FairPlay Canada” coalition calling for mandatory website blocking. This dangerous proposal would put too much control of the internet in the hands of a few, unaccountable corporations, and would result in sweeping censorship and threaten a fundamental pillar of net neutrality in Canada.”

The result of all of this it seems likely that a large number of the submissions to the CRTC have been influenced directly or indirectly by Geist's misleading diatribes against the proposal.²⁴⁰

Greg O'Brien in an insightful article "COMMENTARY: 4,700 people can be wrong" published in [Cartt.ca](http://cartt.ca)²⁴¹ noted how inaccurate and misinformed many of the submissions to the CRTC are. He also adverted to the real problem we as Canadians have in ensuring that debates on important issues do not get subverted by misinformation.

Now, I haven't read each submission, but every single one of the dozens I have read, are wrong. What I see is a lengthy list of people who did not read the FairPlay proposal. So many of the submissions are plainly off topic, have confused facts, or are just blatantly false.

The FairPlay Canada Coalition proposal is not about censorship or network neutrality or freedom of expression or Bell telling everyone what to do. It is about piracy, about foreign operators making money illegally off the backs of others. It's about theft. It's about content makers preserving the freedom to determine how their intellectual property is sold and used – and it's about protecting Canadians from malicious web sites which use IP they don't own in order to attract users and then wreak havoc.

We live in a period where it's incredibly difficult to truly communicate. Oh, there are multiple ways for us all to be in touch so we think it's never been easier to communicate – but ease of access for messages doesn't mean the messages you mean to say are being understood. Clear, honest communications, where people debate and stay on topic? I see less evidence of that daily.

We've all become skilled in obfuscation and avoidance and in changing the topic if we don't want to debate an actual premise. That habit has become so clear, again, since the launch of FairPlay Canada.

Geist tries to deflect his critics by claiming they "rely heavily on character attacks" and not on his arguments on the merits. Geist is accustomed to using *Ad hominem* arguments in support of causes he opposes including in his recent series opposing the proposal where such arguments take up a disproportionate part of his posts. However, this *Ad hominem* argument, at least to the extent it is directed at my prior post, misses my essential claim. My essential claim is that on the merits Geist's arguments simply cannot be supported, as this and my prior blog post contend. However, arguments that bring to the fore Geist's long standing antagonism to copyright protection for the creative community and the types of arguments he habitually makes

²⁴⁰ See, Igor Bonifacic "100,000 Canadians have voiced their thoughts on FairPlay Canada's anti-piracy website blocking proposal", [mobilesyrup](http://mobilesyrup.com), Mar 22, 2018 <https://mobilesyrup.com/2018/03/22/100000-canadians-fairplay-canada/> describing the two websites and the numbers of submissions to the CRTC coming from those sites.

²⁴¹ Feb 15, 2018, <https://cartt.ca/article/commentary-4700-people-can-be-wrong?platform=hootsuite>

to counter effective copyright protection, provides additional context to evaluate his claims. These are not an attack on his character. In this regard, there is a major difference between *Ad hominen* attacks and those premised on similar facts.²⁴²

The proposal should be assessed on its merits based on a careful analysis of the facts and evidence. We should not let widely circulated misinformation be a factor governing decisions about important matters of public policy. If this type of misinformation campaigns are given effect to, we can only expect them to become even more brazen.

17595625

²⁴² See, *Kotylak v. McLean's Agra Centre Ltd.*, 2000 SKQB 383 “Sopinka, Lederman and Bryant, *The Law of Evidence in Canada*, 2nd ed. (Toronto: Butterworth, 1999) deals with the admissibility of similar fact evidence in civil cases. At §11.183, pp. 594-595 the authors state: In civil cases the courts will admit evidence of similar facts if it is logically probative, that is, if it is logically relevant in determining the matter which is in issue; provided that it is not oppressive or unfair to the other side; and also that the other side has fair notice of it and is able to deal with it. Also, *K. M. v. Canada (Attorney General)*, 2004 SKQB 287.