Understanding the Internet as a Human Right

Michael Karanicolas[*]

INTRODUCTION

Around the world, fundamental human rights have undergone a dramatic conceptual shift as a result of the spread of the Internet. The right to freedom of expression, once largely limited to printing, has exploded in a digital world that provides users with an unprecedented megaphone to broadcast their views. The right to political participation and the right to free assembly have similarly been reborn in an age of instant communication, allowing activists to mobilise hundreds of thousands of followers with a single email, text or tweet. Although these are the most notable examples, the Internet has also had a transformative impact on several other recognised human rights, including the right to education, to healthcare and to work.

The Internet's role in the enabling and delivery of human rights has led some to claim that access to the Internet itself should be considered a human right, an idea that has deep implications for both international law and domestic legal frameworks. If, indeed, access to the Internet is a human right, it adds an additional dimension to regulatory issues, since overly restrictive laws that compromise access or damage the vitality or utility of the Internet become more than just bad policy. In some cases, they may constitute violations of international human rights standards.

This Paper discusses the Internet's recognition as a human right and the implications that spring from this recognition in domestic and international law.

I. THE INTERNET'S IMPORTANCE

In order to understand the Internet's importance in the context of human rights, it is useful to consider its increasing centrality to political expression around the world. Political speech is particularly germane because it involves the intersection of three broadly recognised human rights as spelled out in the *International Covenant on Civil and Political Rights* (ICCPR): the right to freedom of expression, the right to freedom of association, and the right to political participation.[1] Although the Internet's specific role in the political process varies depending on each country's level of technological and democratic development, it is just as important as a facilitator of political speech in developing and authoritarian countries as it is in established democracies.

---

* Legal Officer, Centre for Law and Democracy, Halifax, Nova Scotia.

1 International Covenant on Civil and Political Rights, GA Res 2200A (xxi), UNGAOR, 21st Sess, (1966), online: Office of the United Nations High Commissioner for Human Rights <http://www2.ohchr.org/English/law/ccpr.htm>.

(a) The Internet and Political Speech in the Developed World

Give the high international profile of American politics, the United States is a useful starting point in exploring the importance of the Internet in the modern political sphere. Elections in the United States tend to revolve around money, and campaign contributions are treated as a central aspect of political speech.[2] In the course of his 2008 campaign for President, Barack Obama raised over $500 million using online tools,[3] roughly two-thirds of his total campaign budget.[4] In parallel to the Internet's increasingly important potential in terms of fundraising (or perhaps because of it), the Internet has also reshaped the way politicians in the United States campaign. The 2008 Presidential campaign was widely viewed as a watershed moment. In the run up to that election, both major political parties held a "YouTube Debate" where questions were submitted by users uploading videos to the content-sharing website.[5] Webchats with candidates and online networking and advertising have also become standard aspects of campaigns.

This shifting emphasis has transformed the meaning of citizen participation in the political process. The most recognisable image from the 2008 campaign, Shepard Fairey's iconic "Hope" poster, was a product of the Internet. Mr. Fairey found the source photograph by searching Google Images, and then released his modified work through the Internet. Although printed copies were also made, the image's rapid distribution and popularisation were primarily due to its "viral" spread through social media sites. Mr. Fairey's image has since been acquired by the Smithsonian Institution for its National Portrait Gallery. Without access to the Internet (specifically, Google Images) it would have been far more difficult for Mr. Fairey to create the poster, and it would have been practically impossible for his work to have had anywhere near as big an impact as it did.

Although the United States has been at the forefront of the integration of the Internet into the electoral process, it is by no means alone in this regard. Facebook pages, Twitter accounts and web chats have all become standard aspects of political campaigning throughout the developed world.[6]

---

2 This fact predates the Internet by a long margin. See Michael Karanicolas, "Regulation of Paid Political Advertising: A Survey" *Centre for Law and Democracy* (March 2012), online: <http://www.law-democracy.org/wp-content/uploads/2012/03/Elections-and-Broadcasting-Final.pdf>.

3 Jose Antonio Vargas, "Obama Raised Half a Billion Online", *The Washington Post* (20 November 2008), online: The Washington Post <http://voices.washingtonpost.com/44/2008/11/20/obama_raised_half_a_billion_on.html>.

4 Obama's total campaign budget was $745 million, according to Open Secrets, online: OpenSecrets.org <http://www.opensecrets.org/pres08/summary.php?cycle=2008&cid=N00009638>.

5 "Part I: CNN/YouTube Democratic presidential debate transcript" *CNN* (24 July 2007) online: CNN <http://www.cnn.com/2007/POLITICS/07/23/debate.transcript/index.html>; and Mike Huckabee, "Part I: CNN/YouTube Republican presidential debate transcript" CNN (28 November 2007) online: CNN <http://articles.cnn.com/2007-11-28/politics/debate.transcript_1_abortion-rights-debate-candidates?_s=PM:POLITICS>.

6 See, e.g., Sam Stein, "Merkel Announces U.S. Trip Via Twitter, German Press Corps Goes Nuts", *Huffington Post* (6 April 2011) online: Huffington Post

The Internet also facilitates coordinated political activism, including at a global level. In late 2011, the United States Congress began discussing the *Stop Online Piracy Act* (SOPA), which would have granted enormous powers to holders of copyrighted material to shut down websites suspected of infringement, both in the United States and internationally.[7] The proposed bill immediately attracted criticism from the European Parliament,[8] as well as from NGOs, academics and tech companies.[9] However, the most effective protest against the proposed bill was conceived, coordinated and carried out entirely online. On 18 January 2012, over 7,000 websites, including Wikipedia and Reddit, blacked out their services for 24 hours. The protest attracted enormous attention both online and in traditional media, and an estimated 162 million web users viewed the protest banner that replaced Wikipedia's site. By the end of the day, it was reported that several United States Senators who had sponsored the legislation were withdrawing their support, and the bill was shelved shortly thereafter.[10] Political action on this scale is virtually unthinkable without the Internet, while the immediate success of the blackout is a clear demonstration of the power of online protest.

It remains true in the United States, and elsewhere in the developed world, that political speech is possible without access to the Internet. But people who live in the United States — or any other nation where the Internet has established a central place in the political discourse — who do not have access to the Internet are denied full substantiation of their right to freedom of expression. Not only has the Internet expanded and enriched political discourse, but now that a significant and increasing amount of the political process is taking place online, access to the Internet has become a requirement for the full realisation of the right to free expression and to political participation.

<http://www.huffingtonpost.com/2011/04/04/merkel-announces-us-trip-_n_844418.html>; "Dominique de Villepin utilise de plus en plus Twitter pour critiquer le gouvernement", *République Solidaire* (28 December 2011) online: République Solidaire <http://www.republiquesolidaire.fr/9766-dominique-de-villepin-utilise-de-plus-en-plus-twitter-pour-critiquer-le-gouvernement-francetelevisions-28122011/> [in French]; and "David Cameron blames Mumsnet webchat delays on laptop", *BBC News* (19 November 2009) online: BBC <http://news.bbc.co.uk/2/hi/uk_news/politics/8368975.stm>.

7 US, HR 3261, *Stop Online Piracy Act*, 112th Cong, (2011), online: <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261:>.

8 Jennifer Baker, "European Parliament Joins Criticism of SOPA", *PC World* (18 November 2011) online: PC World <http://www.pcworld.com/businesscenter/article/244247/european_parliament_joins_criticism_of_sopa.html>.

9 Declan McCullagh, "Google, Facebook, Zynga oppose new SOPA copyright bill", cnet (15 November 2011) online: cnet <http://news.cnet.com/8301-31921_3-57325134-281/google-facebook-zynga-oppose-new-sopa-copyright-bill/>.

10 "What did Wikipedia's blackout accomplish", *National Post* (19 January 2012) online: National Post <http://news.nationalpost.com/2012/01/19/what-did-wikipedias-blackout-accomplish/>.

(b) The Internet and Political Speech in the Developing World

The Internet is at least equally important as a tool for political participation in repressive countries, as recent uprisings in Iran and the Arab world have demonstrated. In the Iranian case, widespread allegations of vote rigging and fraud during the 2009 Presidential elections saw massive popular protests against Mahmoud Ahmadinejad's purported re-election. Police and pro-government militia responded violently, leading to the deaths of several protesters, which in turn spurred further protests against the brutality, though the uprising was ultimately suppressed. Due to the strong role that social media services played in the protests, the media dubbed the events the "Twitter Revolution."

Anti-authoritarian protests across the Arab world in 2011 and 2012, dubbed the "Arab Spring", were triggered by a Tunisian man's self-immolation in protest against corrupt and arbitrary treatment at the hands of local authorities. This led to a popular uprising in Tunisia against the longstanding and repressive government, and spurred similar protests across the Arab world, most notably in Egypt, Libya, Syria, Bahrain and Yemen.

In both the Iranian and Arab protests, significant attention has been devoted to the role that the Internet, and specifically social media sites such as Twitter and Facebook, played in the uprisings. Although some have expressed scepticism about claims that the protests were coordinated and mobilised online,[11] it is significant that during the Iranian, Egyptian and Syrian uprisings the government responded to the protests by shutting down or drastically reducing Internet service.[12] In the Iranian case, it is also evident that the United States government considered social media to be an important component of the protests, since the State Department took the unusual step of asking Twitter's administrators to delay implementing a planned upgrade that would have cut daytime service to protesting Iranians.[13]

The role of social media in these uprisings further illustrates how online communication can substantiate the right to free expression. In countries where political

---

11 Joel Schectman, "Iran's Twitter Revolution? Maybe Not Yet", *Bloomberg Businessweek* (17 June 2009) online: Bloomberg Businessweek <http://www.businessweek.com/technology/content/jun2009/tc20090617_803990.htm>; "Tunisia protesters use Facebook, Twitter and YouTube to help organize and report", *Los Angeles Times* (14 January 2011) online: Los Angeles Times <http://latimesblogs.latimes.com/technology/2011/01/tunisia-students-using-facebook-and-twitter-to-organize.html>.

12 See Hiawatha Bray, "Finding a way around Iranian censorship", *The Boston Globe* (19 June 2009) online: The Boston Globe <http://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_twitter_web_proxies_to_sidestep_iranian_ censorship/>; Toby Mendel, "Assessment of Media Development in Egypt" *Centre for Law and Democracy* (June 2011) online: <http://unesdoc.unesco.org/images/0021/002146/214638EB.pdf>; and Elizabeth Flock, "Syria internet services shut down as protesters fill the streets", *The Washington Post* (3 June 2011) online: The Washington Post <http://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html>.

13 Sue Pleming, "U.S. State Department speaks to Twitter over Iran", *Reuters* (16 June 2009) online: Reuters <http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616>.

speech is banned or heavily regulated, the Internet is the best (and often the only) way to subvert these restrictions, allowing citizens an avenue to express themselves and to vent their frustrations with comparative anonymity. It also provides protesters with a connection to the outside world. Thanks to the Internet, footage showing the brutality of government crackdowns in Egypt, Iran, Syria, Bahrain and Libya appeared nearly instantaneously on YouTube, mobilising and consolidating public and global opinion against the atrocities. It may theoretically have been possible to smuggle the footage into the hands of journalists through other means, but it would have been far more difficult, slower, more dangerous and less likely to succeed.

For these protestors, the Internet is the only effective mechanism for enabling a right to free expression. This is equally true for bloggers in China, for dissident-journalists in Myanmar or for anyone else living under a regime where the fundamental right to freedom of expression is infringed. An Iranian protester with a working Internet connection will (to a certain degree) be able to exercise their right to free expression. Cut off that Internet connection, and their free expression disappears:

> Even in nations with totalitarian systems, the Internet will offer a kind of fifth column for democratic expression that will be increasingly virulent. Despite the efforts of closed societies to stamp out the Internet, their economic need to go online will inevitably lead to a democratic opening through Internet participation.[14]

In democratic societies the distinction is not quite so black and white, but access to the Internet has nonetheless become inextricably fused with the right to free expression in practice. That is to say, the Internet has added so much to our modern capacity to exercise freedom of expression, in terms of political speech but also of every other aspect of communication — including the arts, socialising and networking, commerce and commercial speech and religious expression — that to be denied access to the Internet is to lose the ability to exercise fully one's right to free expression. The Internet has done so much to expand the practical reality of free expression that its denial can, in some sense, render the right itself hollow, just as the right to express oneself orally but not to print or publish would curtail the right to free expression so much that it would lose an important part of its very meaning.

II. RECOGNITION OF THE INTERNET AS A HUMAN RIGHT

The claim that access to the Internet is a human right is not new. This idea has been recognised, to varying degrees, in several jurisdictions. In 2001 Greece amended its Constitution to include Article 5A, which states:

> 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the

14 Dick Morris, "Direct Democracy and the Internet" (2000-2001) 34 Loy LA L Rev 1033 at 1053.

> State . . .[15]

In France, the Constitutional Council in 2009 struck down a controversial law that would have required ISPs to permanently block Internet access to users accused of copyright violations, in part because the freedom to access online communication services was held to be protected under the Declaration of the Rights of Man and the Citizen of 1789.[16] Although the French decision does not explicitly recognise the Internet as a freestanding right in the way that the Greek Constitution does, this decision was subsequently cited by the Costa Rican Constitutional Court, in a ruling that went considerably further:

> In the context of a society based on information or knowledge, this imposes upon public authorities, for the benefit of those under their administration, to promote and guarantee universal access to these new technologies.[17]

Several jurisdictions have also recognised the fundamental importance of the Internet by imposing legal requirements to ensure universal service, beginning with Estonia, which in 2000 mandated that online access must be "universally available to all subscribers regardless of their geographical location, at a uniform price."[18] Similar requirements have been introduced in Finland,[19] Spain[20] and Nova Scotia.[21]

At the international level, the importance of the Internet was recognised as early as 1999 by the Inter-American Commission on Human Rights:

> [The Internet] is a mechanism capable of strengthening the democratic system, contributing towards the economic development of the countries of the region, and strengthening the full exercise of freedom of expression. Internet is an unprecedented technology in the history of communications that facilitates rapid transmission and access to a multiple and varied universal data network, maximizes the active participation of citizens through Internet use, contributes to the full political social, cultural and economic development of nations, thereby strengthening democratic society. In turn, the Internet has the potential to be an ally in the promotion and dissemination of

---

15 2008 SYNTAGMA [SYN] [CONSTITUTION] 5A (Greece) online: <http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf>.

16 Cons const, 10 June 2009, *Act furthering the diffusion and protection of creation on the Internet*, (2009), 2009-580 DC, online: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf>. The Council later approved an amended version of the law allowing for a maximum cut-off of one year, and which introduced judicial review into the process.

17 Sentencia 12790: Expediente: 09-013141-0007-CO, para V. Unofficial translation by the author.

18 Tel Act, 9 February 2000, s 5.2.2, online: <http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/estonia.htm>.

19 *Communications Market Act*, 363/2011, s 60C(2), online: <http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf>.

20 *Sustainable Economy Act of 2011* BOE 2011, 55.

21 Broadband for Rural Nova Scotia, online: Department of Economic and Rural Development and Tourism <http://www.gov.ns.ca/econ/broadband>.

> human rights and democratic ideals and a very important instrument for activating human rights organizations, since its speed and amplitude allow it to send and receive information immediately, which affects the fundamental rights of individuals in different parts of the world.[22]

The most significant international step towards recognising the right to access the Internet came in 2011, with the adoption of the *Joint Declaration on Freedom of Expression and the Internet* by the special mandates for freedom of expression at the UN, OAS, OSCE and African Commission,[23] which recognised the duty of State to promote universal access to the Internet:

> Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.[24]

There is, thus, a substantial body of law recognising access to the Internet either as a human right or as a vital delivery mechanism for human rights, whose importance in this context is such that it should be considered tantamount to a human right. As the Internet continues to expand its role in people's day to day lives, a role that is already nearly ubiquitous in many countries, there is every reason to expect that this recognition will grow. This raises significant considerations with regards to any regulatory regime whose provisions impact the use and nature of the Internet, by bringing international human rights law into the equation.

III. REGULATING THE INTERNET AS A HUMAN RIGHT

As a medium of communication, it is apparent that any regulation of the Internet must conform to international guarantees of freedom of expression. As the special mandates on freedom of expression stated in their 2011 Joint Declaration:

> 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 (the "three-part" test).[25]

---

22 OAS, Inter-American Commission on Human Rights, *Annual Report of the Inter-American Commission on Human Rights 1999: Report of the Office of Special Rapporteur for Freedom of Expression*, OR OEA/Ser.L/v/II Doc.5 (2011) at c II.

23 The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. Since 1999, these mechanisms have adopted a Joint Declaration annually focusing on a different freedom of expression theme.

24 *Joint Declaration on Freedom of Expression and the Internet* (UN; OSCE; OAS; ACHPR) (1 June 2011), online: OSCE <http://www.osce.org/fom/78309>.

25 *Supra* note 24 at para 1(a).

The three-part test referred to above comes from Article 19(3) of the ICCPR:

> (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights and reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[26]

This means that States can only legitimately impose restrictions on the Internet where such restrictions are set out in a clear legal rule, pursue a legitimate aim, and are necessary in order to protect that aim, which implies that they do not infringe the right to freedom of expression more than is necessary to protect the aim.

Where States engage in overt measures to control the Internet — such as deleting websites or cutting off or reducing service — this clearly engages the right to freedom of expression. This is no different from seizing copies of a newspaper or destroying a publication's presses. However, if the Internet is recognised as a human right, or tantamount to a human right, States' obligations go beyond merely avoiding the active denial of service. Like other human rights, such as the right to education and the right to medical care, States have an active responsibility to promote access to the Internet, and to take steps to protect the nature and character of the Internet in order to preserve its inherent value.

One implication of this is that simply extending regulations designed for other forms of media, such as newspapers or broadcasting, to the Internet are not sufficient because such measures fail to take into account the special nature and value of online communications. This section examines the major regulatory areas impacted by a recognition of the right to the Internet.

(a) Expanding Access

The first and most obvious duty that attaches to States as a result of the Internet's being recognised as a human right is an obligation to work towards universal access. However, the resources that States are able to allocate to extending access to the Internet are dependent on the means at their disposal, taking into account their wealth and level of development. While many countries are currently in a position to institute universal access programmes, the same cannot be said for the world's poorer nations, particularly those with large rural populations. As a result, realisation of the right to the Internet must be subject to progressive implementation goals.

Several jurisdictions, mostly in the developed world, have already instituted programmes to guarantee universal access to broadband Internet. These initiatives are generally funded through a mixture of public and private money, and involve the setting of various benchmarks for required minimum service. In Nova Scotia, the Broadband for Rural Nova Scotia programme, a public-private partnership, guarantees any household that requests it connection to the Internet at a download speed of at least 1.5 mbps, and at a cost that is comparable to what urban customers

---

26 *Supra* note 1.

pay.[27] Finland, which has a universal access programme that is also financed through a combination of private investment and public subsidies, has a benchmark minimum data transfer speed of 1 mbps which must be provided at a "reasonable price".[28] In order to ensure that all residences or businesses are able to connect to the Internet should they later choose to do so, Finland also obliges telecoms companies to extend optical fibre networks or cable networks capable of carrying a transfer speed of at least 100 mbps to within 2 km of every home or business.[29]

The question of what connection speed is necessary to ensure meaningful enjoyment of the right to the Internet is difficult partly because adequate connection speeds are a moving target. As faster connections become the norm, websites are designed with increasingly high requirements for access. As a result, connection speeds that were perfectly adequate ten years ago would struggle to handle many modern websites. However, the larger difficulty in providing a definitive answer to the question of what speed of connection is adequate is that this is dependent on the resources available.

An analogy can be made between the right of access to the Internet and the right to education, another right which is subject to progressive implementation. Education is recognised as a human right in the *Universal Declaration of Human Rights* (UDHR).[30] However, the extent of a State's responsibilities in implementing this right depends on the resources available to it. Article 13(2) of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR) spells out States' responsibilities regarding the right to education:

> The States Parties to the present Covenant recognize that, with a view to achieving the full realization of this right:
>
> (a) Primary education shall be compulsory and available free to all;
>
> (b) Secondary education in its different forms, including technical and vocational secondary education, shall be made generally available and accessible to all by every appropriate means, and in particular by the progressive introduction of free education;
>
> (c) Higher education shall be made equally accessible to all, on the basis of capacity, by every appropriate means, and in particular by the progressive introduction of free education;
>
> . . .
>
> (e) The development of a system of schools at all levels shall be actively pursued, an adequate fellowship system shall be established, and the material conditions of teaching staff shall be con-

---

27 "The Role Model for Sustainable Rural Broadband", Case Study, (2011) online: <http://www.motorola.com/web/Business/_Documents/Case%20studies/_Static%20files/WNS_Case%20Study_Utilities_Broadband%20for%20Rural%20Nova%20Scotia%20Initiative.pdf>.

28 Finland, Ministry of Transport and Communications, *Internet*, online: Ministry of Transport and Communications <http://www.lvm.fi/web/en/internet>.

29 *Ibid.*

30 *Universal Declaration of Human Rights*, GA Res 217(III), UNGAOR, 3d sess, Supp No 13, UN Doc A/810, (1948) 71.

> tinuously improved.[31]

Thus, primary education is a set requirement, but secondary and higher education should be progressively introduced in a non-discriminatory way as far as resources permit. This is reinforced by the language of Article 2(1) of the ICESCR, which states:

> Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.

The specific obligations incumbent upon each State to provide education to its people depends on the resources available to it. As the country develops, those responsibilities increase. In other words, the obligation is not necessarily to provide universal education, but to work towards the provision of universal education, making the best possible use of resources and prioritising its development as befits a human right.

The same can be said of the Internet. Most States may not be in a position to provide all of their citizens with universal access, but a right of access to the Internet means that all States have an obligation to work towards progressive realisation of this goal.

For States where Internet penetration is extremely low and resources are extremely limited, there are other baseline responsibilities that should be addressed. These focus mainly on creating a legal and regulatory environment that encourages the development and use of the Internet. One example might be the need to promote competition by breaking up traditional government monopolies over the provision of Internet services, which have been shown to obstruct the development of the sector.

(b) Copyright and Intellectual Property

Among the most contentious regulatory issues are those surrounding the protection of intellectual property online. Although intellectual property rights holders have a legitimate interest in ensuring that their rights are not violated, several countries have passed or are in the process of discussing laws that take an overly heavy-handed approach to the issue of online piracy, and in doing so threaten to undermine the Internet's character as a free-flowing medium.

One of the most common approaches to regulating online piracy is through "notice and takedown" provisions, such as those found in the United States' *Digital Millennium Copyright Act* (DMCA)[32] or the European Union's Directive on Electronic Commerce.[33] In essence, the notice and takedown system grants content

---

31 *International Covenant on Economic, Serial and Cultural Rights*, GA Res 2200(XXI), UNGAOR, 21st sess, Supp No 16, UN Doc A/6316 (1966) 49.

32 *Digital Millenium Copyright Act*, Pub L No 105-304, 112 Stat 2860 (1998).

33 EC, *Commission 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 Market*, [2009] OJ L 178/1.

hosts immunity from liability for copyright infringement perpetrated by their users provided they act expeditiously to remove the content once notified. In practical terms, the DMCA procedure is that if a copyright owner discovers their material online they must provide the host of the content with notice including information on how to locate and identify the material, a statement of good faith belief that there is no legal basis for use of the work (such as fair use or fair dealing), and a statement of the accuracy of the notice that the complainant is or is authorised to act on behalf of the copyright holder. The host must then remove the content, with a requirement for notification of the individual who perpetrated the alleged infringement after the material has been removed.

The "notice and takedown" system has been criticised for placing an onus on content hosts to enforce copyright claims without proper judicial process. Because their immunity is conditional on speedy compliance, the content hosts generally do not investigate whether the copyright claims are legitimate, or whether the material in question could fall under one of the exceptions to copyright. From a legal perspective, it is safer for them just to comply. Under the DMCA, the problem of false notifications is meant to be addressed through the counter-notice mechanism, whereby the alleged infringer provides notice to the content host of their intent to challenge the removal, along with their consent to refer the matter to an appropriate judicial body. If the copyright owner does not respond to the counter-notice by filing a lawsuit for copyright infringement within 14 days, the ISP is required to restore the material.

Despite these safeguards, there is evidence that DMCA provisions have been abused. In 2008, an organisation presumed to represent the Church of Scientology filed over 4,000 takedown notices with YouTube over a period of 12 hours for videos that were critical of Scientology.[34] Although many users responded with counter-claims, they nonetheless had their content, and in some cases, their accounts suspended while YouTube dealt with the procedure. The Church of Scientology has also used the DMCA to force Google to delist critical websites, though they are by no means the only offender.[35] Creationist groups are known to have employed similar tactics to silence their opponents.[36] The United States District Court for the Northern District of California found in 2008 that Universal Music Corporation had abused the DMCA through a takedown request over a YouTube video.[37] The video contained a clip of children dancing to a song by Prince, the audio of which was of poor quality and which was only audible for about twenty seconds. The Court found that the video so obviously constituted fair use

---

34 Eva Galperin, "Massive Takedown of Anti-Scientology Videos on YouTube" *Electronic Frontier Foundation* (5 September 2008) online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube>.

35 "Google Asked to Delist Scientology Critics (#1)" *Chilling Effects Clearinghouse* online: <http://www.chillingeffects.org/notice.cgi?NoticeID=232>.

36 Bob Beschizza, "YouTube Bans Anti-Creationist Group Following DMCA Claim", *Wired* (16 September 2007) online: Wired <http://www.wired.com/wiredscience/2007/09/youtube-support/>.

37 *Lenz v Universal Music Corp*, 572 F Supp 2d 1150 (ND Cal 2008).

that Universal had acted indiscriminately and in bad faith by filing the takedown.

The DMCA includes sanctions for knowingly abusing the law, which were notably applied in the case of *Online Policy Group v Diebold*.[38] Diebold was a Californian company that manufactured electronic voting machines, which had been criticised after allegations that the machines were faulty. An unknown person published leaked (or possibly stolen) internal emails from Diebold employees that suggested the company knew about the flaws, and relevant quotes from the emails were subsequently duplicated over the Internet. In response, Diebold sent out dozens of letters alleging that the reprinting of the emails was a copyright violation, and demanding that they be taken down. Nearly all of the content hosts complied, but one, the Online Policy Group, fought back alleging that Diebold was abusing the DMCA. The judge found that the republications obviously constituted fair use, and that Diebold could not have reasonably believed that reprinting the emails was a copyright violation. As a result, the court ordered Diebold to pay US$125,000 in damages. Although the *Diebold* case ended with a just resolution, it provides further illustration of the potential for abuse within the notice and takedown system. Dozens of content hosts other than the Online Policy Group complied with Diebold's takedown requests, even though the company did not have a legal leg to stand on.

Critics of the notice and takedown system have advocated a move to a system involving greater due process or, better yet, a system where the Internet service providers' role as policemen is removed entirely. Canada's approach, referred to as "notice and notice", is a good example of this. According to Canada's *Copyright Act*, service providers only have an obligation to pass notices of claimed infringement on to offending users.[39] From there, the dispute is essentially between the user and the copyright holder. Crucially, service providers' immunity is not contingent on their participation in the process. Though they retain discretion to remove offending material, they do not risk liability if they do not.

Given the evidence of abuse within the DMCA, there is a strong argument in favour of systems like Canada's, and one that is bolstered by the recognition of the Internet as a human right. However, in some countries, the political winds appear to favour even harsher anti-piracy laws, including some measures which allow for Internet service to be cut off entirely for users accused of copyright infringement. In France, for example, the Creation and Internet Law establishes a complaints-driven three-strike process for violations of intellectual property.[40] After three complaints about a particular IP address, the web-service provider is required to suspend the user's Internet access services. Significantly, the user is also blacklisted from obtaining Internet access services from any other company for a period of up to a year. A similar three-strike approach to cutting off Internet access was adopted in South Korea with the 2009 revisions to its *Copyright Act*.[41] In the United King-

---

38 337 F Supp 2d 1195 (ND Cal 2004).

39 *Copyright Act*, RSC 1985, c C-42.

40 *Loi nº2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet*, JO, 12 June 2009, 9666.

41 Sun Young-Moon & Daeup Kim, "The Three Strikes Policy in Korean Copyright Act 2009: Safe or Out?" (2011) 6 Wash JL Tech & Arts 171.

dom, the *Digital Economy Act*,[42] passed in 2010, would have empowered the government to block Internet access from any location where copyright was being infringed, or where copyright infringement was being facilitated. The United States' SOPA proposal would have enabled intellectual property rights holders to obtain court orders barring advertisers from doing business with sites that enable or facilitate copyright infringement, and have required search engines and even domain name registrars to delist these sites.[43]

Several of these measures have faced stiff resistance. As mentioned in above, debate over the SOPA bill was put on hold after a massive campaign against its passage. In the United Kingdom, the government halted implementation of the provision of the *Digital Economy Act* that allowed Internet access to be blocked, after a public outcry.[44] Similarly, France's Culture Minister recently described the anti-piracy enforcement of the Creation and Internet Law as "unwieldy, uneconomic and ultimately ineffective", and the French government is launching a consultation to re-examine their approach to copyright infringement.[45]

The recognition of a right to the Internet has important implications for regulatory schemes that allow a blocking of access. It is difficult to see how measures that allow for access to be blocked with little or no due process, or which provide for a reverse onus on users to justify their Internet use, could stand up to the three-part test for restrictions on freedom of expression.

Beyond the regulatory issues noted above, there is a more fundamental question about changing the underlying rules regarding the protection of intellectual property. A balance needs to be found between safeguarding freedom of expression and the open character of the Internet, on the one hand, and providing appropriate protection to intellectual property rights, on the other. However, in finding this balance, the fact that the Internet has fundamentally changed both attitudes towards and realistic possibilities of protection of intellectual property has to be taken into account. It is unrealistic to expect a generation weaned on filesharing to accept a return to the restrictive rules of the past regarding intellectual property. The emergence of the Pirate Party, whose political agenda focuses almost entirely on intellectual property law reform and which now holds seats in the European Parliament, is an illustration of how attitudes are changing.

This does not mean that there should be no protection for intellectual property. Indeed, even the Pirate Party does not advocate this, instead suggesting that copyright terms should be limited to five years.[46] While rights-holders would likely consider this to be unrealistic, current copyright protections, which generally extend either 50 or 70 years beyond the death of the creator, could also be seen as extreme, particularly when contrasted with patents, which generally expire after 20

---

42 *Digital Economy Act 2010* (UK), c 24.

43 *Supra* note 7.

44 "Government drops website blocking" *BBC* (3 August 2011) online: BBC <http://www.bbc.co.uk/news/technology-14372698>.

45 Richard Chirgwin, "France backs away from Hadopi" *The Register* (6 August 2012) online: The Register <http://www.theregister.co.uk/2012/08/06/hadopi_under_fire/>.

46 "International — English — The Pirate Party" online: Piratepartiet <http://www.piratpartiet.se/international/english>.

years.[47] One might also question why copyright protection should persist even after the death of the intended beneficiary, namely the creator. With increasing numbers of copyrights now being held by (immortal) corporations, the "life-of-the-artist" itself has become conspicuously archaic as a yardstick. It is somewhat ironic to hear complaints by rights-holding organisations about how traditional judicial remedies for copyright infringement are ill-equipped to deal with digital piracy, when these same groups are fighting for the maintenance of a system so obviously crafted for an earlier age.

Questions may also be raised as to the scope of copyright protection. The *Diebold* case is a good example of how copyright law has expanded far beyond its original purpose of protecting the livelihoods of artists and writers. Based on this purpose, it is difficult to understand why the internal emails of employees at a manufacturing firm require copyright protection at all.

Some rights-holders have adapted to the shifting ground of the online age. Within the music industry, there has been considerable debate over the implications of filesharing. Although the recording industry is a major lobbyist in favour of tougher anti-piracy laws, many prominent musicians have embraced filesharing as an effective way of marketing their music and connecting with their fans.[48] Others have experimented with new business models, most notably the band Radiohead, which released an album for download by inviting users to pay whatever they thought was appropriate.[49] Other bands have advocated subscription models, where users pay a flat monthly rate that entitles them to download or listen to unlimited material.[50] Time, and the market, will tell if any of these approaches are broadly sustainable in the long term. But by seeking the strict enforcement of traditional copyright law and refusing to acknowledge how the Internet has changed things, major rights-holding organisations risk marginalising their own position. The traditional rules are also increasingly at odds with the fast pace of change and increasing fluidity of information. The spread of the Internet should be viewed as an opportunity for meaningful reform and dialogue about the protection of intellectual property, with a view to arriving at an appropriate balance between the interests of creators and those of the public.

---

47 For further discussion of the onerousness of modern copyright law, see the work of David Vaver, a good introduction to which can be found online: <http://www.slaw.ca/2006/04/25/publishers-and-copyright/>.

48 Steve Hargrave, "Singers Challenge Lily Over Download Debate" *SkyNews* (19 October 2009) online: Sky News <http://news.sky.com/home/showbiz-news/article/15408601>.

49 Angela Monaghan, "Radiohead challenges labels with free album" *The Telegraph* (2 October 2007) online: The Telegraph <http://www.telegraph.co.uk/finance/markets/2816893/Radiohead-challenges-labels-with-free-album.html>.

50 Helienne Lindvall, "Behind the Music: Moguls and musicians thrash out filesharing" *The Guardian* (13 September 2010) online: The Guardian <http://www.guardian.co.uk/music/musicblog/2010/sep/13/behind-the-music-filesharing>.

(c) Net Neutrality

Net neutrality is another major regulatory issue which has been the subject of extensive debate globally, and which must be revisited in considering the Internet as a human right. Without delving too deeply into the technicalities, the debate over net neutrality stems from claims that increasing use of the Internet for bandwidth-intensive activities, such as streaming high-quality video or downloading large files, is straining the capacity of service providers and slowing down the Internet for all users.

Several solutions have been proposed to address this alleged congestion. These include instituting fees per distance that data packets travel,[51] throttling large consumers of bandwidth or users of particular services[52] or, most controversially, the institution of a "tiered" Internet allowing users to pay in order to have their data prioritised.[53] These proposals have been criticised for being contrary to the principle of net neutrality, whereby all Internet traffic is handled in a non-discriminatory fashion.

States have approached this regulatory issue in different ways. In July 2010, Chile became the first country in the world to legally guarantee net neutrality.[54] The EU, after a public consultation between June and September 2010, decided against legislating on the matter, determining that transparency and media scrutiny would be sufficient to keep the Internet free and open. Canada's regulatory agency, the Canadian Radio-television Communications Commission (CRTC) rejected a model based on charging per bandwidth, but decided to permit data throttling on peer-to-peer filesharing networks between 4:30 p.m. and 2 a.m.[55]

Political wrangling around net neutrality continues in the United States, but for the time being the FCC's Open Internet Order governs the issue.[56] The three main rules in the order are a requirement for transparency of network management practices, a prohibition on blocking legal content, and a prohibition on "unreasonable discrimination" of legal content (defined as distinctions that go beyond "reasonable network management"). The precise meaning of this remains unclear, but the explanatory note suggests that while some traffic management to mitigate or reduce congestion may be justified, particularly to prevent heavy-users from crowding out

---

51 Vytautas Valancius et al, "How Many Tiers? Pricing in the Internet Transit Market" (Paper delivered at the ACM SIGCOMM 2011 in Toronto, Canada, 17 August 2011) online: <http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p194.pdf>.

52 *Comcast Corp v FCC*, 600 F 3d 642 (DC Cir 2010).

53 Al Franken, "Net Neutrality is Under Attack . . . Again" *The Huffington Post* (8 November 2011) online: The Huffington Post <http://www.huffingtonpost.com/al-franken/net-neutrality-is-under-a_b_1082225.html>.

54 See Boletín Nº 4915-19, online: <http://www.camara.cl/pley/pley_detalle.aspx?prmID=5300> [in Spanish].

55 "CRTC offers compromise on usage-based billing" *CBC News* (15 November 2011) online: CBC News <http://www.cbc.ca/news/politics/story/2011/11/15/pol-crtc-ubb-decision.html>.

56 US, Federal Communications Commission, *Preserving the Open Internet*, (2011) 76 FR 59192, online: <http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf>.

everyone else, broad-brush throttling measures and premium prioritisation schemes will not be permitted.

Pinning down the ideal regulatory formula is beyond the technical scope of this analysis. But the recognition of the Internet as a human right gives rise to an obligation to adopt a model that allows for the best and most affordable universal access. The claim, made by proponents of a tiered Internet, that increasing profits for service providers is necessary in order to spur further investment which will in turn provide a faster Internet for all users, deserves be investigated along with other claims.[57] However, the Internet's status as a human right means that any scheme which would result in the poor being priced out of the online world, or which would reduce connection speed and utility among the rural or disadvantaged, should be rejected.

In framing the debate on which regulatory model will provide the best service, it is also important to stress that net neutrality should be considered separately from online copyright infringement. In the course of the 2007 FCC inquiry into broadband industry practices, the Motion Picture Association of America (MPAA) submitted a comment that, "Any policy efforts relating to Net Neutrality must promote the protection of intellectual property."[58] To the contrary, legitimate traffic management regulations should focus solely on providing a faster and more effective Internet for all users.

(d) Defamation

A lot of judicial attention, including at the international level, has been devoted to achieving a proper balance between protecting reputations through defamation law and ensuring respect for freedom of expression. As a result, a number of international standards on this have been widely recognised. These include the idea that defamation should be a matter for the civil, rather than the criminal, law, based on the idea that criminal defamation laws cannot be justified as "necessary" given that civil laws provide adequate protection for freedom of expression.[59] Similarly, remedies for defamation should be proportionate, and a written retraction or apology or a small monetary payout should usually suffice, unless the victim can show he or she has suffered real monetary damage. Public bodies should not be permitted to sue for defamation, since free and open criticism of their work is an important part of the democratic process. Public officials do have the right to bring defamation cases to protect their reputations, but the law should reflect the fact that their position means that they are required to tolerate a greater degree of criticism.

---

57 Arshad Mohammed, "Verizon Executive Calls for End to Google's 'Free Lunch'" *The Washington Post* (7 February 2006) online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html>.

58 *Re Broadband Industry Practices*, WC Docket No 07-52, online: <http://apps.fcc.gov/ecfs/document/view?id=6519529325>.

59 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression (December 2002), online: <http://www.cidh.oas.org/relatoria/showarticle.asp?artID=87&lID=1>.

All of these standards, established to deal with offline statements, are equally applicable to the Internet.

However, the Internet has given rise to new issues regarding defamation law. First, because defamation is based on harm to one's reputation, defamation suits could traditionally be filed in any jurisdiction where such harm was caused, which generally meant anywhere the harmful material was distributed. However, material published on the Internet can be accessed anywhere in the world. This gives rise to an enormous potential for "forum-shopping" in online defamation suits. Well-financed litigants can file suit in jurisdictions where laws are most favourable to them.

This demonstrates the need to rethink the concept of jurisdiction as applied to defamation. Subjecting all online comments to a vast patchwork of different standards for defamation is impractical and would chill speech by forcing writers to adopt a "lowest common denominator" approach whereby all expression must be crafted to avoid liability in those jurisdictions which are most restrictive with regards to freedom of expression.[60] It could also lead to people erecting "walls" to prevent their speech from being accessible from countries with problematic defamation laws, curtailing the Internet's borderless character. A good solution to this problem was proposed in the 2005 Joint Declaration of the (then) three special international mandates on freedom of expression — the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and the OAS Special Rapporteur on Freedom of Expression — which focused on the internet:

> Jurisdiction in legal cases relating to Internet content should be restricted to States in which the author is established or to which the content is specifically directed; jurisdiction should not be established simply because the content has been downloaded in a certain State.[61]

Another issue which requires rethinking in the Internet age is the traditional understanding of harm. This idea is rooted in a village context of reputation and honour (early defamation laws were adopted mainly to try and prevent duelling). However, traditional understandings of reputation do not necessarily correspond to the freewheeling world of online discussion.

This problem is illustrated by the United States case of *Bock v Scheff*.[62] Carey Bock had hired Sue Scheff's company to help her with a family issue and, unhappy with the services she received, Ms. Bock posted negative comments about Ms. Scheff and her company in an online forum for parents with troubled kids. Ms. Scheff sued Ms. Bock for defamation and, when Ms. Bock neglected to contest the suit (she subsequently claimed to have been unable to afford a lawyer), Ms. Scheff was awarded more than US$11 million in damages. There is a clear difference be-

---

60 Toby Mendel, *Mapping Digital Media: Online Media and Defamation* (London, UK: Open Society Foundations, 2011), online: <http://www.soros.org/initiatives/media/articles_publications/publications/mapping-digital-media-online-defamation-20110503/ online-media-and-defamation-20110503.pdf>.

61 Joint Declaration on Freedom of Opinion and Expression (UN; OSCE; OAS) (21 December 2005), online: OSCE <http:www.osce.org/fom/27455>.

62 991 So 2d 1043 (Fla 4th Dist 2008).

tween Ms. Bock as an individual venting her frustrations online and a newspaper publishing a damning exposé of a particular business. The former is far more likely to be taken with a grain of salt. However, as this case illustrates, civil law (at least in the United States) has yet to take this distinction into account. The chilling effect of judgments like this, which subject every critical comment made on every message board to massive potential liability, and their potential to undermine the ability of the Internet to stimulate public debate, are obvious.

This is not to say that defamed parties should be denied any remedy. Indeed, the growing importance of online advertising and commerce means that one's online reputation is important and often commercially valuable. But there are other appropriate remedies that are better suited to the online context. One example is the right of reply, whereby aggrieved parties are given a chance to respond in the same manner in which the defamatory material was disseminated. Long a staple of printed media, the right of reply is even more appropriate when applied to an online context since the democratisation of discourse is the essence of the Internet. Although the exorbitant size of the settlement is why *Bock* stands out, there is a reasonable argument that the entire case was unnecessary since Ms. Bock's comments were posted on a public message board where Ms. Scheff was free to respond on equal terms. Absent demonstrable material harm (such as the loss of a valuable client as a result of a posting), there is no discernible reason why netizens should not be allowed to decide for themselves who is in the wrong after hearing both sides of the story.

Traditional understanding of publication and republication is also ill-suited to the online context. In many countries, every republication of a defamatory statement constitutes a new act of defamation. But online publication is in effect continuous, and laws need to be adapted to accommodate this. Furthermore, even printed references to defamatory statements can be considered as separate acts of defamation.[63] This means that merely hyperlinking to a defamatory statement can lead to liability, a state of affairs which obviously undermines the free exchange of information online.

This ties into the issue of liability for ISPs or websites for hosting or publishing defamatory material. In the United States, the *Communications Decency Act of 1996*[64] provides broad immunity to any "interactive computer service" such that they are not considered publishers when handling material produced entirely by third parties. In *Barrett v Rosenthal*,[65] this immunity was found to extend to deliberate acts of republication by web users. The defendant in that case, Ilena Rosenthal, came across a letter on the Internet which contained false information about Dr. Stephen Barrett, a psychiatrist notable for campaigning against alternative medicine and health fraud. She proceeded to repost the letter on two alternative medicine newsgroups. Ultimately the California Supreme Court ruled she had immunity since she had neither authored nor edited the letter in question.

This approach differs from that in several other jurisdictions which have yet to revisit their defamation laws. In Argentina, Google and Yahoo! have been sub-

---

63 *Lindley v Delman*, 25 P 2d 751 (1933).

64 *Communications Decency Act of 1996*, 47 USC §230.

65 40 Cal 4th 33 (2006).

jected to numerous injunctions ordering them to remove search engine links to allegedly defamatory material.[66] Some judgments have also ordered the search engines to remove all links to "similar sites". In the EU, the Directive on Electronic Commerce provides absolute protection for mere conduits of information. Hosts of user-generated content are protected so long as they remove material once they are aware of its defamatory nature, or of facts pointing to this.

The similarity between this process and the notice and takedown procedures applied to copyright infringement have produced similarly problematic results, whereby content hosts take an overly cautious approach for fear of losing their immunity. This is exacerbated by the complexity of defamation law, as well as the enormous potential costs of losing a case (or even fighting one). Once again, in establishing a proper standard it is instructive to examine the 2005 Joint Statement of the three special international mandates on freedom of expression:

> No one should be liable for content on the internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.[67]

More broadly, in order to properly adapt defamation law to the Internet age it is important to understand that defamation is a highly contextual concept. Many variables can be considered in determining whether a statement is defamatory, including the identity of the complainant and the author, the intentions of the author, the nature and tone of the allegation, the source of information upon which the statement is based, the public interest and urgency of the subject and whether or not the author contacted the complainant prior to publishing it. These and other variables are taken together in order to weigh whether or not the public interest in freedom of expression and open debate outweighs the private harm to reputation that the statement caused. From this perspective, it is reasonable to suggest that the standard of defamation must also be considered in light of the medium of communication employed. As a forum for public debate, the Internet provides users with unprecedented freedom to engage, fostering lively debate on issues large and small. There is a clear public interest in a regulatory system that will maintain this state of affairs. Just as defamation cases against newspapers often consider reasonable professional standards, such that the letter of the law not constrain journalists from doing their job, laws involving online commentary must evolve in a manner that maintains the value of the Internet as an open space, and considers the specific parameters in which online publishers, authors and content hosts operate.

(e) Other Content Restrictions

Content filtering, widely seen as an inappropriate system for protecting against illegal content, is already carried out in many countries. While restrictions at the national level can occasionally be justified — for example where they are designed to locate and block off the spread of computer viruses — any such measures must meet strict requirements of necessity and proportionality. It is clear, for example,

---

66 See Eduardo Bertoni & Elizabeth Compa, "Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad" *Derecho Comparado de la Información* (July — December 2010) 25.

67 *Supra* note 61.

that broad brush filtering of the type carried out by the Chinese government is not acceptable as a restriction on freedom of expression under international law. The Chinese measures include restrictions on searching for particular news items, such as the Tiananmen Square protests, or the blocking off of entire websites, notably many human rights organisations such as Amnesty International. Although China's "Great Firewall" is the best known example, they are far from the only country that carries out widespread Internet censorship.

In addition to the requirements of necessity and proportionality, another important ingredient is transparency. While blocking off a particular website might occasionally be justified, such as a site wholly dedicated to promoting racial violence in a region where there was a real risk of such violence taking place, governments should be open and transparent about any and all censorship measures. For instance, users attempting to visit a blocked website should be presented with a message stating that the website has been blocked, rather than a generic error message.

The universality of the Internet also means that broad content restrictions, particularly if combined with liability for material deemed offensive or harmful, runs the same risk described above of forcing publishers and creators into a "lowest common denominator" approach of ensuring all content meets the most restrictive standards. Even without liability, traditional means of censorship, such as blocking potentially offensive material at the border, are problematic in an online context since a Balkanisation of the Internet would undermine its universal and globalising power. As a result, governments should be wary of imposing the same strict standards on online content that they might consider appropriate for printed or broadcast material, since greater leeway is the price of keeping the Internet free and open.

Content restrictions designed to address the problem of spam are a particularly difficult issue. Anti-spam measures are necessary to conserve bandwidth and to protect users from intrusive mass marketing. Far from being a mere annoyance, the unrestricted proliferation of spam constitutes a threat to the Internet's value and character. However, there are difficulties in defining just what constitutes spam and in striking a balance between controlling true spam and overbroad measures. Canada's anti-spam law, which requires users to expressly opt-in to receiving emails unless there is an existing business relationship, provides an interesting model in this area.[68]

(f) Data and Privacy Protection

Another vital measure to ensure that users trust online communications, which is key to the use of the Internet as a medium for enabling freedom of expression, is the protection of user privacy. This applies to private sector actors, such as Internet service providers and commercial websites, as well as to government.

The ins and outs of online privacy have been the subject of voluminous scholarly research. What is relevant to this analysis is the understanding that the value of

---

68 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying our commercial activities*, SC 2010, c 23.

the Internet as a vehicle for the rights to free expression, association and political participation is significantly dependent on users' feelings of anonymity. The protests in Iran and in the Arab Spring occurred in the context of highly repressive regimes, where political expression is a dangerous business. The Internet allowed young dissidents to congregate and develop solidarity, and the protesters felt confident in participating in this political discourse because of their perceptions of the Internet as an anonymous space. Take away that anonymity, and the Internet's value as a forum for open discourse is diminished.

The importance of anonymity to the candour of online debate is not limited to repressive nations. When TechCrunch.com, a popular web forum for the discussion of technology products, changed its format to one which required users to attach their real name to any comments left, they found that the site, which had been known for hosting blistering criticism of sub-standard products, lost its scathingly honest character.[69] The importance of anonymity to online expression was recognised by the Council of Europe Declaration on Freedom of Communication:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas (. . .) States should respect the will of users of the Internet not to disclose their identity.[70]

Limitations to online privacy are commonly found in both civil and criminal legislation. On the criminal side, some degree of surveillance by the authorities can be justified as necessary for protecting national security, or for stopping cybercrimes such as the spread of child pornography. However, these laws can be difficult to craft given their potential to trench on human rights. In early 2012, the Canadian government proposed legislation that would have required service providers to log information about all customers' Internet use, as well as allowing police to access personal information about users without judicial oversight. When the proposal attracted widespread protest, Public Safety Minister Vic Toews responded by claiming that opponents of the measure were supporting child pornographers.[71]

There is also a tension between online anonymity and the rules on defamation and intellectual property since, in some instances, protection of reputation and property rights is possible only where anonymity is lifted. Once again, finding the right balance for the online world can be difficult.

Several jurisdictions have already put in place excessively intrusive measures to undermine anonymity on the Internet. Italy requires all users of cyber cafés to

---

69 Podcast of Tom Standage & Martin Giles, *The Economist* (16 November 2011) online: The Economist <http://www.economist.com/blogs/babbage/2011/11/babbage-november-16th-2011>.

70 Council of Europe, Committee of Ministers, *Declaration on Freedom of Communication on the Internet* (2003), online: Council of Europe <https://wcd.coe.int/ViewDoc.jsp?id=37031>.

71 Ivor Tossell, "Toews's 'child pornographers' gaffe aside, Bill C-30 has real dangers" *The Globe and Mail* (21 February 2012) online: The Globe and Mail <http://www.theglobeandmail.com/news/technology/digital-culture/ivor-tossell/toews-gaffes-aside-bill-c-30-has-real-dangers/article2344551/>. The full text of the proposed bill can be found at: <http://parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965>.

register with a photo ID, and requires the managers of these cafés to track the websites each user visits.[72] These rules place Italy in the same category as Syria when it comes to Internet monitoring, with both countries claiming that the measures are necessary to fight terrorism.[73] The Egyptian Telecommunication Regulation Law also infringes on user anonymity by forbidding the use of any encryption technologies without written permission from the telecommunications regulatory authority, the armed forces, or the national security entities.[74] Although the post-revolutionary government claimed to have been "looking into" changing this provision, it has yet to be changed at the time of research.

In South Korea, popular websites are now required to collect the names and national identification numbers of users before they can post comments or upload content.[75] This change was part of a package contained in the Cyber Defamation Law, passed in an attempt to combat cyber-bullying following two high-profile suicides. While cyber-bullying is a serious problem, this case illustrates the problem with passing new laws as a reaction to the worst cases. The Cyber Defamation Law had an immediate negative effect on Internet speech, among other things leading Google to block users registered as South Korean from uploading or commenting on videos. Although the YouTube ban is easily circumvented (South Korean users merely need to shift their registration setting to a different country), the move nonetheless demonstrates the skittishness of content providers in the face of overly intrusive legislation, and the way that laws challenging online anonymity can damage the web environment. As a general rule, governments need to take care when responding to dramatic incidents, and to resist knee-jerk calls for new legislation, without paying sufficient attention to whether or not they erode fundamental freedoms.

It is also important for privacy protections to extend to personal information collected by private sector operators, in particular those operating for commercial gain. A key issue here is informed consent, with consumers being presented with clear and easily understandable information on how their data will be used and shared before they provide it. This should include a right to review and correct data, as well as to withdraw consent for the use of data, otherwise known as a right to be forgotten.[76] All of these rules should be subject to an effective complaints and

---

72 Sofia Celeste, "Want to check your email in Italy? Bring your passport" *The Christian Science Monitor* (4 October 2005) online: <http://www.csmonitor.com/2005/1004/p07s01-woeu.html>.

73 Lester Haines, "Syria orders cybercafe owners to ID customers" *The Register* (14 March 2008) online: The Register <http://www.theregister.co.uk/2008/03/14/syria_cybercafe_measure/>.

74 *Egypt Telecommunication Regulation Law*, Law No 10 of 2003, Art 64, online: <http://www.tra.gov.eg/uploads/law/law_en.pdf>.

75 Martin Williams, "Google Disables Uploads, Comments on Youtube Korea", *PC World* (13 April 2009) online: PC World <http://www.pcworld.com/article/162989/google_disables_uploads_comments_on_youtube_korea.html>.

76 David Zax, "Europe, Data, and the 'Right to Be Forgotten'" *technology review* (25 January 2012) online: technology review <http://www.technologyreview.com/blog/helloworld/27525/?p1=blogs>.

enforcement mechanism to ensure that users continue to view the Internet as a safe space for candid conversation.

CONCLUSION

The benefits of a free flow of information and ideas over a universally accessible Internet have long been extolled. Analysing the regulation of the Internet from a human rights perspective, however, gives rise to a set of conclusions that, if largely in line with a benefits-based analysis, are conceptually distinct. More than just a new frontier to be developed, the online world becomes an essential part of the human experience, and one which governments around the world have a duty to nurture and protect.

Regardless of whether one accepts or rejects the recognition of a human right to access the Internet, the Internet's emerging status at the core of universally recognised human rights means that much more thought needs to be given to how to design regulatory approaches which strike an appropriate balance between protecting legitimate interests — such as intellectual property, reputation and combating crime — and an unhindered flow of information. This paper is far from the first to note the problems with applying traditional regulatory approaches to the Internet, but far less thought has been given to designing new approaches that will better suit an online world.

The purpose of this paper is not to provide answers to all the questions that arise as a result of analysing regulation of or access to the Internet from a human rights perspective. Rather, it seeks to frame the issues so as to help ensure that we are asking the right questions. It seeks to move the debate forward by providing an outline of the major regulatory, legal and policy issues that require further research, and by posing some of the key questions that such research, along with policy development work, should seek to answer.