Report on Cybercrime Laws and Digital Content Restrictions in Myanmar[1]

January 2017

1. Background: Human Rights and the Internet

In the decades since its inception, the Internet has become a key delivery mechanism for a range of human rights, most obviously freedom of expression, but also the rights to association, to education, to work and to take part in cultural life, among others. The enormous impact of the Internet was noted in 2013 by Navi Pillay, then the UN High Commissioner for Human Rights, who said:

> Modern technologies are transforming the way we do human rights work. In 1993, the World Wide Web was just four years old, and its future use and reach could barely have been imagined, nor how fundamentally the Internet would affect our lives. Together with social media and IT innovations, these technologies are dramatically improving real-time communications and information-sharing. They are also magnifying the voice of human rights defenders, shining a light on abuses, and mobilizing support for various causes in many parts of the world.[2]

As a consequence of the Internet's transformative power, questions about how to interpret and apply human rights in an online context have become central to modern understandings of these rights. An important starting point to understanding human rights and the Internet is to establish that human rights standards apply to the online world. In June 2012, the UN Human Rights Council noted that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the

---

[1] Drafted by Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy, for the Myanmar Media Lawyers' Network.

[2] Navi Pillay, United Nations High Commissioner for Human Rights, 20-20 Human Rights Vision Statement for Human Rights Day, 10 December 2013. Available at: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14074.

Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[3] The UN General Assembly affirmed this in a 2013 resolution.[4]

Beyond merely establishing that rights exist online, the Internet's importance to human rights has led to calls for access to the Internet itself to be recognised as a human right, specifically as part of the right to freedom of expression.[5] An increasing number of human rights mechanisms, at both the national and international level, either expressly or implicitly recognise that Internet access is a right, and that measures to restrict or deny Internet access are a serious human rights challenge. Among the earliest statements in support of this can be found in Greece's Constitution, as amended in 2001, which stated in part:

> 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 State…[6]

Using similar language, the Constitution of the Mexican state of Colima protects access to the information society.[7] In 2000, Estonia's parliament passed a law declaring that Internet access was a fundamental human right of citizens.[8] A right of access to the Internet, along with a concomitant duty on the State to promote and guarantee access, was also recognised by Costa Rica's Constitutional Court in a 2010 ruling.[9] An increasing number of jurisdictions impose universal service obligations on Internet access providers including Finland,[10] Spain[11] and the Canadian province of Nova Scotia.[12]

---

[3] Resolution A/HRC/20/L.13, 29 June 2012. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.

[4] Resolution A/C.3/68/L.45/Rev.1, 26 November 2013. Available at: www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

[5] Centre for Law and Democracy, *A Truly World-Wide Web: Assessing the Internet from the Perspective of Human Rights* (Halifax: Centre for Law and Democracy, 2012). Available at: www.law-democracy.org/wp-content/uploads/2010/07/final-Internet.pdf.

[6] Article 5A(2). Available at: www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf.

[7] Article 1(IV). Available [in Spanish] at: info4.juridicas.unam.mx/adprojus/leg/7/218/.

[8] Colin Woodard, "Estonia, where being wired is a human right", Christian Science Monitor, 1 July 2003. Available at: www.csmonitor.com/2003/0701/p07s01-woeu.html.

[9] Sentencia 12790: Expediente: 09-013141-0007-CO, para. V. Available [in Spanish] at: 200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=TSS&nValor1=1&nValor2=483874&strTipM=T&lResultado=1&pgn=&pgrt=&param2=1&nTermino=&nTesauro=&tem1=&tem4=&strLib=&spe=&strTem=&strDirTe.

[10] Communications Market Act, 363/2011, s. 60C(2). Available at: www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf.

[11] Sustainable Economy Act of 2011, Article 52. Available [in Spanish] at www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf.

[12] Michael MacDonald, "Eastlink gets rural broadband deadline", Canadian Press, 20 February 2014. Available at: www.cbc.ca/news/canada/nova-scotia/eastlink-gets-rural-broadband-deadline-1.2545211.

The 2011 *Joint Declaration on Freedom of Expression and the Internet* by the special international mandates for freedom of expression[13] also highlighted States' duty 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.[14]

While the right to freedom of expression has long been understood to impose a positive obligation on States to promote a robust expressive environment,[15] it is relatively novel for access to a particular technology or means of communication to be considered a human right. The recognition noted above therefore signals the radical and transformative potential of the Internet as a communicative medium. Furthermore, a significant groundswell of support underlies this position. A BBC World Service poll in 2010 found that 79 percent of people around the world believe that access to the Internet is a fundamental right.[16]

2. Challenges to Regulating Speech Online

The spread of the Internet has been accompanied by challenges in developing new legislation, and adapting existing legislation. There is, without question, a pressing need for governments around the world to draft laws which enable full advantage to be taken of the digital transition. While some legal frameworks can easily either be applied directly in an online context or be applied with only minor changes, others require substantial adaptation. It is, in this context, critically important to ensure that any legislation which impacts on freedom of expression is consistent with recognised international human rights standards. This is particularly important since a significant part of the Internet's value as an expressive medium flows from its open and borderless nature, qualities which can only be preserved through a light regulatory touch. In order to fully harness the power of the

[13] 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.
[14] 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.
[15] See, for example, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, para. 66. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[16] See: "Internet access is 'a fundamental right'", BBC, 8 March 2010. Available at: news.bbc.co.uk/1/hi/technology/8548190.stm.

Internet, with all of the economic, cultural and expressive benefits which that entails, people must be allowed to communicate freely online.

This does not mean, of course, that the Internet should be a lawless or unregulated place. However, it is important for regulatory authorities to carefully consider the impact that proposed legislation may have. This is particularly true in countries with relatively low rates of Internet access, where the potential for poorly drafted legislation to create a chilling effect, whereby individuals steer well clear of the potential zone of application to avoid censure, is magnified due to the relative novelty of the medium. As of June 2016, there were only 11 million Internet users in Myanmar, which is around 19% of the population.[17] This may be compared with Thailand, where around 60% of the population uses the Internet, or Canada, where the figure is 93%.

The key is to avoid laws which criminalise normal or innocuous online behaviours, which impose excessively harsh sanctions or which are vague and open to misapplication. The adoption of such laws at this stage could permanently stunt the development of a thriving online community in Myanmar, thereby denying the country the full level of economic, cultural, social and developmental benefits that the Internet has the potential to provide. Unfortunately, some of Myanmar's laws, in particular the Electronic Transactions Law and the Telecommunications Law, fail to meet international human rights standards.

3. Cybercrime Laws

One of the less positive impacts of digital life is the emergence of a new class of digital crimes, such as online fraud and cyberstalking. Several countries have passed cybercrime legislation with the aim of combating these threats. When considering such laws, it is important to take into account the fact that many online crimes are not as new as they may seem. Fraud, for example, is already a crime in most countries. While enforcement techniques and definitions may need to be updated to cope with this evolving class of behaviours, there is often no reason for the creation of entirely new crimes to counter these threats. Particularly concerning is a trend among some countries to pass new legislation which imposes particularly harsh penalties on crimes committed online, as compared to their offline equivalents. It is difficult to justify why the mere use of the Internet in the commission of a crime should warrant a more severe punishment. In developing new cybercrime legislation, lawmakers should therefore ask themselves, first, whether the creation of the new criminal offences which are envisaged is even necessary and, second, whether the punishments imposed are proportionate and consistent with existing legal and human rights standards.

[17] See: www.internetworldstats.com/asia.htm.

Where new legislation is necessary, it is also important to define the prohibited behaviours carefully. Drafting processes should include input from technical experts, as well as from the human rights community and other key stakeholders, to ensure that innocuous or benign behaviours are not also covered by the law. As often as not, these kinds of mistakes are the result of a lack of expertise among policymakers, who may not fully understand the scope and nature of online communications.

4. Defamation Online

The faceless nature of online interactions often makes users more uninhibited in what they are willing to say. There are positive aspects to this. For example, when debating matters of public interest, encouraging people to express opinions which are unpopular or which challenge conventional wisdom is a social benefit. The flipside to this is that online conversations may spiral into becoming more aggressive or abusive, or people may feel more comfortable making threats or defamatory statements.

Just as human rights apply to the Internet, so too do laws regulating speech. Defamation is no more acceptable an online context than offline. However, while it is legitimate to create and enforce rules to protect reputations, international human rights standards require defamation to be a matter for the civil rather than the criminal law. This is based on the idea that criminal defamation laws cannot be justified as "necessary" given that civil laws provide adequate protection for freedom of expression.[18] According to a September 2011 General Comment by the UN Human Rights Committee, the official body responsible for overseeing States' compliance with their ICCPR obligations:

> States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty.[19]

Many democracies – including East Timor, Georgia, Ghana, Sri Lanka, the United Kingdom and the United States – have rescinded their criminal defamation laws, while others have done away with the possibility of imprisonment for defamation. There is no evidence to suggest that this has led to any increase in the publication of defamatory material. If a less intrusive measure, namely a civil law prohibition on defamation, is effective in protecting reputations, a more intrusive measure, i.e. criminal defamation, cannot be justified.

[18] 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. Available at: www.cidh.oas.org/relatoria/showarticle.asp?artID=87&lID=1.

[19] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 47.

Another widely recognised principle of defamation law, which is equally applicable to the digital world, is that remedies for defamation should be limited and proportionate. 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 losses, for example where their business was directly impacted. This, along with the principle that defamation laws should be civil in nature, implies that under no circumstances is it justifiable to impose custodial sentences for defamation, because such oppressive sanctions are simply not necessary to protect reputations.

Another key standard regarding defamation is that 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.

5. The Electronic Transactions Law and the Telecommunications Law

Considered in light of the standards spelled out in the previous sections, there are some problems with Myanmar's Electronic Transactions Law, under which several cases have been brought stemming from comments made online.

Section 33(a) of the Electronic Transactions Law stipulates that any person found using electronic technology to do "any act detrimental to the security of the State, or the prevalence of law and order, or community peace and tranquillity" may be punished by a minimum of seven years imprisonment. Section 38 further extends this penalty to anyone who "attempts to commit" any offence, or "conspires" or "abets" in the commission of any offence under the Act.

This provision is far too broad to be justifiable according to international human rights standards, since the terms "security of the State" and "community peace and tranquillity" are not defined, and could extend to a wide range of legitimate criticism and other activities. Furthermore, criminalising all speech which is deemed to be "detrimental" to security or law and order is unduly restrictive and fails to strike an appropriate balance between freedom of expression and security/order. Writing an article accusing the police of using poor criminal investigation techniques might be considered to be detrimental to order, but it is clearly perfectly legitimate.

The fact that Section 38 functionally extends this prohibition to anyone who conspires or abets in the commission of an offence further broadens this law's already unacceptably wide applicability, potentially extending liability to, for example, a social network on which critical views were expressed or even telecommunications companies whose infrastructure facilitated the

communications. The interconnected nature of online networks even means that virtually every telecommunications provider in the country could be charged for their complicity in helping to distribute messages which are found to violate the provisions of the Electronic Transactions Law. This is likely emblematic of a point raised earlier, namely that legislation may be poorly drafted due to a lack of expertise among lawmakers. It is unlikely that lawmakers intended to extend liability to virtually every Internet service provider for messages which they have no practical means of removing or filtering out. However, even if the law is not enforced in this manner, its existence and the serious criminal risks which the sector formally faces as a result of it, are very problematical.

Section 33(b), which provides for criminal penalties for anyone who receives, sends or distributes information "relating to secrets of the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture", is also very problematical. Generally speaking secrecy laws which criminalise the *receipt* of information raise freedom of expression concerns. Leaks are an increasingly common part of the global discourse and often perform a vital public function, which is recognised in whistleblowing laws. It is one thing to impose penalties on those who breach a computer system to obtain information or who share information beyond its authorised recipients (i.e. the person who is responsible for the leak). But journalists should be allowed to receive and report on information they receive from third parties without fear of prosecution. Furthermore, by explicitly including distributors, section 33(b) also covers telecommunications providers and other online platforms even more directly than section 33(a), so that the problems noted above also apply here.

Section 33(b) also fails to recognise the important role of whistleblowing, which can be vital to preventing corruption, environmental damage or threats to health and safety. These sorts of disclosures are generally unauthorised and nearly always delivered electronically. The need to safeguard whistleblowers is in line with Article 33 of the United Nations *Convention Against Corruption*, which calls on States to consider incorporating protections into their legal system for people who disclose information about corruption "in good faith and on reasonable grounds."[20]

Section 34(b), which criminalises the "intercepting of any communication within the computer network, using or giving access to any person of any fact in any communication without permission of the originator and the addressee", is also problematical. This would appear to criminalise the common, and completely benign, practice of forwarding emails unless both the originator and addressee have given permission for this, which is extremely rare.

[20] General Assembly Resolution 58/4 of 31 October 2003, entered into force 14 December 2005, available at: https://www.unodc.org/unodc/en/treaties/CAC/.

Perhaps the most problematical provision of the Electronic Transactions Law, and the one which has led to several high profile and abusive prosecutions, is section 34(d), which criminalises "creating, modifying or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person".

Myanmar's Penal Code already provides for up to two years' imprisonment for defamation. There is no need, therefore, for a separate defamation rule in the Electronic Transactions Law. At the most, it might be necessary to tweak the Penal Code to make it clear that the defamation provisions there apply to digital communications. As noted above, the Penal Code is already excessive according to international human rights standards, which hold that defamation should be a civil matter and that prison sentences are never an appropriate remedy for defamation. However, section 34(d) is significantly more problematical than the Penal Code provisions. It is far broader, applying to any statement which lowers a person or organisation's dignity or is detrimental to their interests, and provides for an even harsher penalty, namely up to five years' imprisonment. It also fails to incorporate any of the defences for defamation found in the Penal Code, such as when a statement is true.

Many of the problems noted above with the Electronic Transactions Act are also present in the Telecommunications Law. This includes duplicate or unnecessary offences. For example, section 66(c), which criminalises "[s]tealing, cheating, misappropriating or mischief of any money and property by using any Telecommunications Network", is unnecessary given the existing Penal Code provisions dealing with theft.

The Telecommunications Law also contains yet another criminal defamation provision, section 66(d), under which problematical prosecutions have been launched in Myanmar. This provision is even broader than the one in the Electronic Transactions Act, since it also applies to material which is "disturbing". There can often be a high public interest to the dissemination of "disturbing" material, such as a videotape exposing police brutality. Section 66(d) also prohibits material which causes "undue influence", an extremely vague definition which could potentially apply to emotive poetry or particularly persuasive essays.

Section 68(a), which prohibits the "communications, reception, transmission, distribution or conveyance of incorrect information with dishonesty or participation", is also significantly overbroad, as it seemingly criminalises any electronic communications which are not fully truthful. Given the number of online terms of service agreements which require users to certify that they have read and understood them. Given the frequency with which most people click through these without looking at them, let alone reading and understanding them, this would criminalise virtually everybody who has used the Internet.

Section 73 of Telecommunications Law also applies the same penalty for all of these offences to anyone who abets in their commission, meaning that, like the Electronic Transactions Law, it extends liability to virtually every Internet service provider or online platform.

6. Intermediaries and Online Speech

In addition to the legislative challenges to protecting human rights on the Internet, another challenge is the enormous role that private sector intermediaries play in providing access to, managing, facilitating and mediating online speech.

Although States bear the primary obligation for ensuring respect for human rights, it is now recognised that private sector actors also have a direct responsibility to respect and to foster respect for human rights. Rather than creating a platform for an influential few, as newspapers or broadcasters do, Internet intermediaries facilitate speech directly by individuals, giving everyone a platform and access to a global audience. By the same token, however, this grants these intermediaries an unprecedented influence over individuals' right to freedom of expression and access to information. This power has also attracted the attention of State actors, which are placing increasing pressure on online intermediaries to facilitate and/or participate in human rights violations, for example by supporting intrusive surveillance systems or by policing user content.

In recent years, there has been an increasing focus on the human rights implications of the policies and practices of intermediaries. The most high profile work on human rights and the private sector in general is the 2011 *Guiding Principles on Business and Human Rights*, [21] which was developed under the auspices of the United Nations. In 2016, the Centre for Law and Democracy published its own comprehensive guide to human rights standards for private sector online intermediaries, *Stand up for Digital Rights: Recommendations for Responsible Tech*.[22]

7. Other issues

Another unique aspect of the Internet is its truly global nature, with material uploaded anywhere being instantaneously available to users anywhere. This gives rise to issues about jurisdiction in legal cases relating to Internet content. This has been a particular problem in relation to defamation, with plaintiffs engaging in what has come to be known as libel tourism, whereby they seek a plaintiff friendly

[21] UN OHCHR, Guiding Principles On Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 16 June 2011, HR/PUB/11/04. Available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[22] Available at: responsible-tech.org/wp-content/uploads/2016/06/Intermediaries-Print.pdf.

jurisdiction in which to bring cases. To address this, the special international mandates for freedom of expression called for the following approach in their 2011 Joint Declaration:

> Jurisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State. Private parties should only be able to bring a case in a given jurisdiction where they can establish that they have suffered substantial harm in that jurisdiction (rule against 'libel tourism').

The Internet has also given rise to new, technologically based control systems, such as filtering and blocking systems. While filtering systems can enhance the ability of end users to exercise control over the content that comes across their desks, filtering or blocking systems imposed by the State represent an unjustifiable form of prior censorship. In their most extreme forms – of which the most famous and pervasive of these is China's "Great Firewall" although similar systems are being explored or implemented in several States, including Russia, Ethiopia and Kazakhstan – these systems also pose a major structural threat to the nature of the Internet. China's Great Firewall not only limits the ability of Chinese people to use the Internet, it also undermines the ability of Internet users everywhere to communicate with people in China.

Another important Internet issue is the principle of net neutrality. At a minimum, this rules out discrimination in the treatment of Internet traffic. As the special international mandates noted in their 2011 Joint Declaration: "There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application." The question of differential charges for carriage and receipt of material over the Internet is more controversial. While some advocates call for this to be prohibited, differential charging has already started to take root and it seems unlikely that it will disappear completely.

The spread of the Internet also poses a challenge to the established system of protection of copyright and intellectual property. The Internet has facilitated a tremendous flowering of creativity and the birth of new art forms. However, it has also led to unprecedented levels of copyright infringement, due to the ease with which digital files can be copied and shared. While the rights of artists to earn a living, including through digital sales, should be safeguarded, States should ensure that exceptions to copyright (such as fair use or fair dealing) are interpreted broadly and in a manner that is appropriately adapted to the digital era. They should also take care to avoid imposing overly harsh penalties for infringement, with cutting off access to the Internet begin a particularly unreasonable measure.

8. Conclusion

Developing a legislative framework to regulate online speech is undoubtedly a tricky and delicate endeavour, and one which is made even more challenging by the complexity, technical sophistication and rapidly evolving nature of the Internet. However, these challenges mean that civil society engagement is of paramount importance to ongoing legislative drafting and reform efforts. Making sure that the concerns of a range of stakeholders are taken into account can avoid clumsy and technically ineffective rules, as well as laws which prohibit innocuous or benign behaviours along with harmful ones. Engagement is particularly important for legal and technical experts who may possess expertise and skill sets that lawmakers do not or who may offer insights and perspectives that are otherwise absent. Myanmar's legal community, of course including the MMLN, has an important role to play in this regard by pushing back against any problematical new laws which are proposed and by pushing for reform of existing problematical laws, such as the Electronic Transactions Law and the Telecommunications Law.