Myanmar: Regulating Digital Content[1]

December 2017

1. Introduction

The Internet provides an increasingly essential underpinning in the modern world for a range of human rights. This includes, most obviously, freedom of expression and access to information, but the Internet is also key to the realisation of such rights as freedom of association, access to education and medical services, and exercising the right to vote in an informed manner. It is widely accepted that human rights standards apply to digital communications tools. The UN Human Rights Council has noted: "[T]he 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 Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[2]

In addition, an increasing number of both international and national human rights systems have recognised that access to the Internet is a human right and that measures to restrict or deny access to the Internet therefore represent an interference with a human right. The Human Rights Council expressed this sentiment in June 2016 when it highlighted:

---

[1] Prepared by Portia Karegeya, Legal Officer, Centre for Law and Democracy, and Toby Mendel, Executive Director, Centre for Law and Democracy.

[2] 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. This was confirmed by a UN General Assembly resolution. See 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.

> [T]he importance of applying a comprehensive human rights-based approach when providing and expanding access to the Internet and for the Internet to be open, accessible and nurtured by multi-stakeholder participation.[3]

The same resolution also condemned:

> [M]easures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law.[4]

The 2011 Joint Declaration on Freedom of Expression and the Internet by the special international mandates for freedom of expression at the United Nations, Organisation of American States, Organization for Security and Co-operation in Europe and African Commission[5] highlighted that States have a 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.[6]

The same Joint Declaration made it clear that regulation of the Internet must conform to general international standards regarding restrictions on freedom of expression:

> 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).[7]

The three-part test comes from Article 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR),[8] a treaty ratified by 169 States as of October 2017, which states:

> (3) The exercise of the rights provided for in paragraph 2 of this article [guaranteeing freedom of expression] carries with it special duties and

[3] Resolution A/HRC/32/L.20, 27 June 2016. Available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/L.20
[4] Resolution A/HRC/32/L.20, 27 June 2016. Available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/L.20.
[5] 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 mandates have adopted a Joint Declaration annually focusing on a different freedom of expression theme.
[6] 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.
[7] *Ibid*.
[8] UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976. Article 19(2) guarantees freedom of expression.

> 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.

States may therefore only legitimately impose restrictions on digital content which are set out as clear legal rules, which pursue a legitimate aim and which are necessary to protect that aim.

When States impose unduly restrictive measures to control content on the Internet – such as blocking websites or filtering content – this is analogous to seizing newspapers or blocking broadcasts, and it therefore represents a restriction on the right to freedom of expression. Furthermore, extending regulatory measures designed for other communications mediums, such as newspapers or broadcasting, to the Internet does not provide adequate protection to the right to freedom of expression because the special nature of the Internet has to be taken into account when designing regulatory measures. As the special mandates stated in their 2011 Joint Declaration:

> Approaches to regulation developed for other means of communication – such as telephony or broadcasting – cannot simply be transferred to the Internet but, rather, need to be specifically designed for it.

There are a number of special features of the Internet. These include, for example, that one can be anonymous online, which fosters open debate and unprecedented frankness. The Internet is also fully global in nature, so that it allows anyone to 'speak to the world' with very modest resources. It is also increasingly accessible, even to poorer citizens of the word. Importantly, the Internet also has the ability to support new, democratic public spaces for debate (virtual public squares). The importance of these spaces in a democracy needs to be taken into account when considering legal or regulatory measures which limit freedom of expression online. These same qualities, however, give rise to regulatory challenges such as difficult jurisdictional issues and questions about where the appropriate limits to free speech lie.

This report focuses on rules in the legal framework of Myanmar which restrict the content which may be created and shared through digital communications tools. It analyses those rules based on international standards in this area and provides recommendations for reform where the rules fail to conform to those standards. The next section of this report outlines some key international standards regarding regulation of digital content, while the following sections evaluate various problematical content restrictions in the Electronic Transactions Law, Official Secrets Act, Telecommunications Law, News Media Law and Penal Code. In many cases, these provisions do not conform to international standards and, in those cases, we recommend that they be repealed or appropriately amended to bring them into line with minimum standards regarding the right to freedom of expression.

2. Freedom of Expression and the Regulation of Online Speech

To derive the maximum economic, cultural and expressive benefits from the Internet, it is imperative that people be allowed to interact and communicate freely online. This does not mean that States may not regulate the Internet, but great care is warranted when doing so in order to preserve the important expressive value of the Internet, which is based, among other things, on its open and borderless nature.

Any legislation or other rules that impact freedom of expression, including content restrictions on digital speech, should be consistent with recognised international human rights standards. As noted above, this means that any restrictions on content should meet the following three-part test:

1. The restriction should be provided by law.
2. The restriction should aim to protect one of the following interests, namely respect for the rights or reputations of others, national security, public order, public health or public morals.
3. The restriction should be 'necessary' to protect that interest.

According to a September 2011 General Comment by the UN Human Rights Committee (HRC), the official body responsible for overseeing States' compliance with their ICCPR obligations, to meet the first standard, a law must be "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly" and it must also be publicly accessible and not confer undue discretion on those charged with applying it.[9] Unduly vague restrictions or restrictions which grant excessively discretionary powers of application to authorities fail to meet the main purpose of the 'prescribed by law' part of the test, which is to grant the power to restrict freedom of expression only to the legislature. In addition, unduly vague rules give way to a wide range of possible interpretations. This falls short of the democratic requirement that individuals be given reasonable and clear notice of exactly what is prohibited so they can regulate their behaviour accordingly.[10]

As far as the 'necessary' criterion, under international law this includes four key elements. First, there must be a pressing or substantial need for the restriction; minor threats do not pass this threshold test for restricting freedom of expression. Second, the approach taken must be the least intrusive manner of protecting the legitimate aim. If alternative measures would accomplish the same goal in a less intrusive manner, the measure chosen is clearly not necessary. Third, the restriction must impair the right as little as possible in the sense that it is not 'overbroad'. Fourth, a restriction must be proportionate. Proportionality is assessed by weighing the likely effect of the restriction on freedom of expression against its benefits in terms of the legitimate aim being

[9] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 25.
[10] Centre For Law and Democracy and International Media Support, *Briefing Note Series: Freedom of Expression* (2014), pp. 5-6. Available at: http://www.law-democracy.org/live/wp-content/uploads/2012/08/Briefing-notes.full-version.Eng_.pdf.

protected. If the harm to freedom of expression outweighs the benefits, the restriction is not justifiable.[11]

States often seek to extend rules governing the dissemination of content offline to the digital world. Some such restrictions translate relatively easily and directly into a digital context or require only minor changes. Others, however, require more substantial adaptation due to differences in the ways information is disseminated digitally. Authorities must carefully consider the impact, sometimes unintended, that proposed rules may have on the flow of information over the Internet. This is perhaps particularly important in Myanmar, where poorly drafted or overreaching legislation could potentially create a significant chilling effect, as individuals steer well clear of potential zones of application of the law to avoid any possible risk of censure.

In many cases, existing content restrictions are already defined sufficiently flexibly to apply in a digital setting. In such cases, States should not create new restrictions, and especially not restrictions which impose harsher punishments, for the online world. Unfortunately, despite the self-evident truth of this, many States have indeed gone ahead and created unnecessary duplicate crimes for the Internet.

Where new content restrictions are indeed necessary due to the different ways that content is disseminated digitally, it is important to define what exactly is prohibited and who exactly is responsible for this very carefully. This is because, due to the wide range of different sorts of online behaviours, it is all too easy to capture innocent or non-harmful activity in rules that are not drafted with an understanding of how people act online. To help prevent this, technical and human rights expertise should be brought to bear on drafting processes, and civil society should be given an opportunity to provide input at an early stage.

Two contentious areas of digital regulation are cybercrime and defamation, for both of which Myanmar has already introduced legislation. Cybercrimes take place online but are not necessarily novel. Rather, in many cases they are simply online manifestations of offline criminal behaviour which does not require new legal treatment. While enforcement techniques and approaches may need to be updated in order to cope with evolving behaviour, there is often no need to create new crimes to counter these threats. Too many countries have already followed the emerging trend of seeking to impose extra harsh penalties when crimes are committed online. This is rarely legitimate. The mere use of a digital tool in the commission of a crime does not mean that a more severe punishment is warranted; this would only be the case where the very fact of the crime taking place online somehow made it more harmful or serious.

It is legitimate to adopt legislation that protects the reputation of individuals, known as defamation laws, and such laws should apply online as well as offline. However, international human rights law imposes some important conditions on defamation laws. First, defamation ought to be a matter for the civil rather than

[11] *Ibid.*, pp. 6-7.

the criminal law; criminal defamation laws cannot be justified as "necessary" given that civil laws provide adequate protection for reputation.[12] At the very minimum, imprisonment should not be imposed as a sanction for defamation. According to the 2011 General Comment by the UN Human Rights Committee:

> 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.[13]

Indeed, remedies for defamation should always be proportionate, even in the case of civil defamation laws. A written retraction or apology or a small monetary pay-out will usually suffice to repair the harm to reputation, unless the plaintiff can show that he or she suffered real monetary losses, for example because of a direct impact on his or her business. Furthermore, according to international standards, public bodies should not be permitted to sue for defamation because free and open criticism of their work is an essential underpinning of democracy. While public officials have the right to bring defamation cases to protect their reputations, the fact that they hold public position of power means that they should be required to tolerate a greater degree of criticism than ordinary citizens.

3. The Electronic Transactions Law

The main goal of Myanmar's Electronic Transactions Law 2004[14] is to facilitate e-commerce, which is of course an important goal. However, some of its provisions also restrict digital content. Sections 33(a) and (b) provide for imprisonment of between 7 and 15 years for any person who uses electronic technology, respectively, to do "any act detrimental to the security of the State or prevalence of law and order or peace and tranquillity or national solidarity or national economy or national culture" or to engage in "receiving or sending and distributing any 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".

These provisions are highly problematical for a number of reasons. The overarching issue is that they are vastly overbroad. No definitions are included in the legislation which might narrow the scope of application of these provisions. This leaves terms such as "security of the State" and "prevalence of law and order" susceptible to a wide range of interpretations, some more legitimate than others. While it is, of course, legitimate to impose certain restrictions on free speech to protect national security and public order, criminalising all speech that may be deemed to be "detrimental" to these

[12] 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.

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

[14] 30 April 2004. Available at: http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan041197.pdf.

interests is unduly restrictive. Such a rule might, for example, be used to prevent reporting on crime or terrorist attacks on the grounds that it might encourage terrorism. In their 2008 Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, the special international mandates on freedom of expression stated: "The public has a right to know about the perpetration of acts of terrorism, or attempts thereat, and the media should not be penalised for providing such information."[15]

Furthermore, sections 33(a) and (b) go beyond just protecting national security and public order to also protect a number of interests – including 'national solidarity', 'national economy, 'national culture', and 'community peace and tranquillity' – that are not recognised as legitimate grounds for restricting freedom of expression in Article 19(3) of the ICCPR. While we might hope that citizens would support these values, the right to freedom of expression applies not only to speech which is popularly welcomed but also to information and ideas which "offend, shock or disturb the State or any other sector of the population."[16]

Section 38 extends these prohibitions to anyone who conspires in or abets the commission of an offence. This potentially extends liability to, for example, the operator of a social network which disseminated prohibited statements or even telecommunications companies whose infrastructure facilitated their distribution. Of course it is unlikely that this was the intention of those who drafted the Law or that authorities would enforce it in this manner. However, the potential for significantly overbroad application of this rule remains problematical.

Section 33(b) deals with the receiving, sending or distributing of State secrets (as noted above, defined unduly broadly). Subject to certain protections (see below), it is legitimate to impose penalties on officials who leak genuinely secret information which they received due to their official functions. However, secrecy laws which criminalise the mere receipt of information raise serious freedom of expression concerns. On the one hand, the fluid flow of information through digital technologies means that almost anyone could be the innocent recipient of secret information, and they should certainly not be penalised for this. On the other hand, it is legitimate for journalists not only to receive but also to further disseminate leaks, and this serves an important function in ensuring that information of public interest reaches the public. As the special international mandates on freedom of expression stated in their 2004 Joint Declaration:

> Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately secret information under their control. Other individuals, including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information.[17]

[15] 10 December 2008. Available at: http://www.osce.org/fom/66176.
[16] *Handyside v. United Kingdom*, 7 December 1976, Application No. 5493/72, para. 49 (European Court of Human Rights).
[17] 6 December 2004. Available at: http://www.osce.org/fom/66176.

Some degree of protection should also be extended to those who leak public interest information, even if they are officials. Leaks serve as an important information safety value in society, often ensuring that information of vital public interest is disclosed, and this is recognised in whistleblowing laws. To ensure that information about wrongdoing, both by public officials and by those working in the private sector, is exposed, there is broad international recognition of the need to offer formal legal protection to whistleblowers, namely those who release information about persons or organisations engaging in illegal, irregular, dangerous, unethical or harmful practices.[18] Whistleblowers require legal protection against reprisals because they often work within the very power structures which are responsible for the problematic behaviour. At a minimum, section 33(b) should include a public interest override, so that those who leak information would be protected where this was in the overall public interest.

Perhaps the most problematical provision in the Electronic Transactions Law is Section 34 which punishes, with a prison term of up to 5 years, anyone who engages in:

> (a) sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer programme dishonestly;
>
> (b) 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;
>
> (c) communicating to any other person directly or indirectly with a security number, password or electronic signature of any person without permission or consent of such person;
>
> (d) 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.

Section 34(a) criminalises a number of actions (sending, hacking, modifying, altering, destroying, stealing and so on) undertaken in relation to "electronic records", "electronic data" and "computer programmes". A "computer programme" is not defined, while electronic data or records are defined as records or information generated, sent, received or stored by means of electronic, optical or other similar technologies. This essentially encompasses all digital content and is, as a result, very widely applicable.

Section 34(a) is problematical because the key word defining the criminal intent – namely 'dishonestly' – is not defined. This could capture a lot of routine online behaviour that is not harmful in any way. For example, if an individual modifies

[18] Thus, Article 33 of the United Nations *Convention Against Corruption* 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." 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/.

an image he or she found online to create protest art in a way that does not violate copyright (say because it falls within the exceptions to copyright), would this be an offence under this provision? What if someone deleted a file which someone else wanted to preserve, something almost everyone has done? This provision is also problematical inasmuch as it repeats an existing criminal offence – stealing – which is already addressed in sections 378- 382 of Myanmar's Penal Code[19] in a way which is sufficient to address the theft of electronic property.

Section 34(b) is also problematical as it appears that even the common, and completely benign, practice of forwarding emails unless both the originator and addressee have given permission for this, which is rare, is criminalised. Worse still is section 34(d), which has already led to some high profile and abusive prosecutions. This provision 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". The scope of protection here – against any detriment to one's interests or any lowering of one's dignity – is simply far too broad. In particular, it completely fails to respect international standards regarding defamation, which have been carefully crafted to represent an appropriate balance between freedom of expression and protection of reputation.

Sections 499-502 of Myanmar's Penal Code already provide for up to two years' imprisonment for defamation, and there is no need for a separate, far more crudely defined, defamation rule in the Electronic Transactions Law. Even the Penal Code provisions are problematical from the perspective of international law, both because they provide for imprisonment for defamation and because they fail to provide for some internationally recognised exceptions. Section 34(d) of the Electronic Transactions Law is significantly more problematical inasmuch as it is far broader – applying to any statement which lowers a person or organisation's dignity or is detrimental to their interests – and it 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, for example true statements.

Finally, 34(c) also fails to take into account the reality of the digital world. It prohibits any communication to any third party containing, among other things, a "security number, password or digital signature" without the consent of the owner. In practice, this happens every day when people forward on emails or other messages containing this sort of content. It may be noted that even if intent is read into these provisions, that would not protect users since they will clearly have had the requisite intent to do the prohibited communication.

Recommendations:

[19] Myanmar Penal Code of 1860 (Indian Act XLV. 1860). Available at: http://www.wipo.int/edocs/lexdocs/laws/en/mm/mm004en.pdf.

- The terms "security of the State" and "prevalence of law and order" in sections 33(a) and (b) should be carefully and narrowly defined to limit the scope of these provisions and the term "detrimental" should be replaced with a more exigent term, such as "intentionally cause harm to".
- The other grounds for restriction in sections 33(a) and (b) – including "national solidarity", "national economy", "national culture", and "community peace and tranquillity" – should be removed.
- Section 33(b) should be limited in scope to cases where an official intentionally leaks legitimately secret information. In addition, a public interest override should apply even in this cases, so that no liability would ensue where disclosure of the information served an overriding public interest.
- Section 34(a) should be amended to: a) define a "computer programme"; b) define the "dishonesty" intent requirement to make it clear that an intent to cause harm to a third party is required; c) define the terms hacking, modifying, and altering; and d) repeal the duplicate offence of stealing. In addition, defences should be added to these provisions to prevent their application to ordinary or regular online behaviour.
- Section 34(b) should be amended to remove the term "using or giving access to any person of any fact in any communication without permission of the originator and the addressee".
- Section 34(c) should be amended to avoid criminalising the forwarding of signatures and the other content covered unless this is done with the specific intent of causing harm to the owner of that content.
- Section 34(d) should be repealed in its entirety.
- Section 38 should be amended to apply only where a person specifically intends to cause the prohibited result.

4. The Official Secrets Act

The Official Secrets Act, 1923,[20] is now nearly 95 years old and is sorely in need of substantial revision or potentially even complete revocation. Section 3(1)(c) provides for imprisonment of up to three years for any person who, for a purpose which is prejudicial to either the safety or interest of the State, "obtains, collects, records or publishes or communicates to any other person any secret official code or password, or any sketch, plan, model, article or note, or other document or information which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy". This increases to up to fourteen years if the offence is related to the "work of defense, arsenal, naval, military, or air force establishment, station, mine, minefield, factory, dockyard, camp, ship or aircraft or otherwise in relation to the naval, military or air force affairs of the State or in relation to any secret official code".

[20] 2 April 1923. Available at: http://www.myanmarconstitutionaltribunal.org.mm/lawdatabase/sites/default/files/myanmar_code/2015/06/19-1923%20THE%20BURMA%20OFFICIAL%20SECRETS%20ACT.pdf.

This is significantly overbroad. First, it is not confined to security but covers any "interest" of the State, which might be deemed to cover practically anything. Second, it is not limited to secret information but includes any information which might be, even indirectly, useful to any enemy. The fact that a flood or other natural disaster had caused significant damage in a country would meet this standard.

Article 19(3)(b) of the ICCPR makes it clear that expression may be limited to protect national security and public order. However, Article 19(3), as interpreted by official bodies, also requires laws restricting free speech to be clear and narrow. Unfortunately, there has been a tendency of both laws and decision-makers in many countries to define national security far too broadly.[21] Guidance on the scope of national security can be found in the *Global Principles on National Security and the Right to Information* (Tshwane Principles), which is the leading international statement in this area.[22] Principle 9 provides a list of categories of information that might legitimately be withheld, in the context of right to information requests, on grounds of national security. This includes: defence plans, operations, and capabilities; production, capabilities or use of weapons systems; measures to safeguard the territory of the State; critical infrastructure or critical national institutions; the operations, sources and methods of intelligence services; and national security information provided by a foreign State.

In addition, international human rights standards require that before punishment may be imposed for speech causing harm to national security or public order, the individual in question must have had a clear intent to cause that harm (i.e. the expression must have been intended to incite imminent violence). Thus, Principle 6 of *the Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, a precursor to the Tshwane Principles, set out the key test for restrictions on freedom of expression in the name of national security:

> Expression may be punished as a threat to national security only if a government can demonstrate that:
>
> (a) the expression is intended to incite imminent violence;
>
> (b) it is likely to incite such violence; and
>
> (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.[23]

This requirement is missing from section 3 of the Official Secrets Act.

---

[21] Centre For Law and Democracy, Toward a Media Regulatory Reform in Middle East and North Africa: Workshop on Criminal Restrictions on Media Content, 24-25April 2014, *Beirut: Background Paper: National Security and Terrorism*. Available at: http://www.law-democracy.org/live/wp-content/uploads/2014/05/National-Security-and-Terrorism.pdf.

[22] Open Society Foundations, *Global Principles on National Security and the Right to Information* (Tshwane Principles) (2013). Available at: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

[23] Article 19, *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* (1995). Available at: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.

Section 5 is also very problematical. It creates various offences relating to "any person" (i.e. not just officials). Section 5(1), for example, covers any "document or information which relates to or is used in a prohibited place or relates to anything in such a place". It is clear that this extends very far beyond information which is sensitive on national security grounds. Pursuant to section 5(1)(c), it is an offence simply to retain such information. According to section 5(2), it is an offence voluntarily to receive any information in contravention of the Act. Section 5(3) prohibits the communication of any information relating, among other things, to "munitions of war", regardless of any impact this might have on national security.

These provisions are not only vastly overbroad on their face, covering a large amount of information that has little or nothing to do with national security. They also contravene the principle, noted above, whereby third parties should not be held liable for communicating, let alone just receiving, confidential information.

Finally, none of the provisions in the Official Secrets Act are subject to whistleblower protections or even a public interest override.

Recommendations:

- The whole Official Secrets Act should be carefully reviewed and amended to bring it into line with international standards. In particular:
  - Section 3 should be revised to limit its application to information which is legitimately secret on national security grounds and to provide for individual sanctions only where an individual acts with intent to cause harm and that harm is likely to result.
  - Section 5 should be revised to limit its scope to officials and, as with section 3, to legitimately secret national security information.
  - A public interest override should be added to the Act.

5. The Telecommunications Law

Like the Electronic Transactions Act, the 2013 Telecommunications Law[24] serves a number of important public goals, including to modernise telecommunications, to protect consumers and to promote universal access to services. At the same time, there are a number of problems with the Telecommunications Law. For example, several offences unnecessarily duplicate pre-existing rules. As an example of this, section 66(c) makes it a crime, subject to a penalty of up to three years' imprisonment, to engage in "[s]tealing, cheating, misappropriating or mischief of any money and property by using any Telecommunications Network". As is the case with the Electronic Transactions Law, the existing Penal

[24] 8 October 2013. Available at: http://www.burmalibrary.org/docs23/2013-10-08-Telecommunications_Law-en.pdf.

Code already has provisions dealing with theft and the misappropriation of property (see sections 403-404).

The Telecommunications Law contains yet another criminal defamation provision, in section 66(d), and several high profile and very problematical criminal prosecutions have already been launched under this provision in Myanmar, leading to a number of convictions. Specifically, the provision provides for a penalty of up to three years' imprisonment for:

> Extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network.

This provision is arguably even broader than section 43(d) of the Electronic Transactions Act, since it applies to any material which is "disturbing", in addition to content which is defamatory. This is very problematical because there is often a high public interest in disseminating material that might be considered "disturbing". For example, a videotape exposing police brutality might be considered to meet this standard.

Section 66(d) is also very problematical inasmuch as it prohibits the dissemination of material which causes "undue influence". The Penal Code already covers extortion (sections 383-389), threats and criminal intimidation (sections 94, 503 and 507), and wrongful restraint and imprisonment (sections 339-348). Section 66(d) fails to define the notion of "undue influence" in the context of telecommunications, leaving it extremely vague and open to potentially overbroad interpretation. For example, the dissemination of emotive poetry, particularly persuasive essays or high-powered advertisements could all be deemed to create undue influence. The Penal Code contains a number of provisions dealing with the offence of undue influence, but these are restricted to particular situations, such as exercising undue influence over officials (sections 162 and 163) or specifically in the context of elections (sections 171C and 171F).

Section 68(a) prohibits the "communications, reception, transmission, distribution, or conveyance of incorrect information with dishonesty or participation". While it may, superficially, seem appropriate to prohibit the dissemination of incorrect information, leading courts in a number of countries have held that blanket prohibitions on 'false news' represent a breach of the right to freedom of expression. In practice, such rules are almost always used for political reasons rather than to protect the public. Thus, in 2000, the Supreme Court of Zimbabwe stuck down a false news provision as being unconstitutional, calling it a violation of the right to freedom of expression.[25] The requirement that the dissemination has to be accompanied by "dishonesty" or "participation", whatever the latter may mean, provides virtually no protection given that it is completely undefined.

[25] *Chavunduka and Choto v. Minister of Home Affairs & Attorney General*, 22 May 2000, Judgment No. S.C. 36/2000 (Supreme Court of Zimbabwe). Available at: http://crm.misa.org/upload/web/CHAVUNDUKA.pdf.

These provisions are particularly problematical in the digital communications environment, given the rapid nature of communications interactions. A perhaps trite example of participating in the dissemination of incorrect information is the action of clicking the "I have read and understood these terms" button that we all do from time to time, given the large number of terms of service agreements which require users to certify that they have read and understood them, implying informed consent. The vast majority of users click these buttons without having read the terms, thereby formally disseminating incorrect information. As a result, this provision would criminalise virtually everybody who has used the Internet.

Section 69 prohibits the disclosure of encrypted information to any "irrelevant person" unless authorised to do so by a court, which can attract a penalty of imprisonment for up to one year. Once again, this is far too broad and fails to contain any defences or limitations. Many people now routinely use encryption to protect their communications, and it is also common for the recipients of that information to pass it on to third parties, which would be rendered criminal by this provision (since it is not limited to official systems of encryption). Indeed, strictly speaking pursuant to this provision, even the originator of an encrypted communication could not authorise its being passed on to a third party, since this power vests only in a court. In any case, rules like this on secrecy of information are legitimate only if they are restricted to information which is genuinely sensitive, whereas this applies whenever information is (merely) encrypted, which is not at all the same thing.

Section 73 of Telecommunications Law applies the same penalty for all of these offences to anyone who abets in their commission so that, like the Electronic Transactions Law, it potentially extends liability to virtually every Internet service provider and social media platform.

Section 75 grants the government vast powers to obtain telecommunications information from private service providers, stating:

> The Union Government may, as may be necessary, direct to the relevant organization for enabling to obtain any information and telecommunications which causes harm to national security and prevalence of law without affecting the fundamental rights of the citizens.

This provision is highly problematical for a number of reasons. First, the terms "as may be necessary" and "harm to national security" are undefined and hence potentially too broad, and so should be narrowed. As noted above, in relation to the Official Secrets Act, while national security may justify some restrictions on freedom of expression, it needs to be defined carefully in order to comply with international human rights law. In the absence of any specific constraints, this provision effectively grants the government broad powers to compel telecommunications companies to conduct potentially intrusive surveillance and even to police and control user content. The potential danger of this was noted in the 2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> Given that Internet services are run and maintained by private companies, the private sector has gained unprecedented influence over individuals' right to freedom of expression and access to information. Generally, companies have played an extremely positive role in facilitating the exercise of the right to freedom of opinion and expression. At the same time, given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression.[26]

Theoretically, the fact that these activities are conditioned on not affecting fundamental rights should provide some protection against abusive behaviour, and this provision is welcome. However, this is a very general clause and it is unlikely that it would be used to impose real constraints on government action under this provision. Instead, what is needed is clear and precise conditions for the exercise of this power, such as an imminent threat of serious harm to a specific national security interest.

Section 77 gives the relevant ministry the power, when an "emergency situation arises", and in the public interest, to direct a telecommunications service provider "to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments." These are, once again, vast and highly intrusive powers. While they are subject to certain constraints – namely that there be an emergency situation and that the measure be in the public interest – these are extremely vague (no definition of either an emergency or the public interest is given) and are unlikely to constrain the use of this provision much. Instead, as with section 75, specific conditions should be incorporated directly into the provision.

Suspending a communications service, whether for one individual or for a section of the public, is an extreme measure. The special international mandates on freedom of expression stated, in their 2011 Joint Declaration, that a general cutting off of Internet services was never justified:

> Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds.[27]

Section 77 also allows for wide intercept powers, the problems with which are discussed just above. And giving the State the power to control telecommunications services is even more draconian in nature.

In addition to limiting the substantive scope of these powers, at the very minimum a number of procedural protections need to be added so as to ensure

---

[26] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27 (16 May 2011), para. 44. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[27] 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

that the due process rights of users are respected. The provision contains no procedural or notice requirements, no indication of how long a suspension, interception or State takeover of services might last, and no other indication of how a measure under this provision might be rolled out. In addition, such measures should be imposed in a transparent manner, subject to requirements of secrecy based on national security, and this is again not provided for. As a result, in its current form this provision fails to meet the requirements of necessity and proportionality.

Recommendations:

- Section 66(c) should be repealed in its entirety as it simply duplicates pre-existing offences. If necessary, the Penal Code could be amended to take into account changes wrought by digital telecommunications systems.
- Similarly, Section 66(d) should be repealed because parts of it are just unnecessary, while other parts are repetitive of Penal Code offences. At a minimum, the offences of defaming, disturbing, causing undue influence or threatening should be removed.
- Section 68(a) should again be repealed. If there is a specific context where the dissemination of incorrect information needs to be prevented, this could be incorporated into a new provision (preferably in the Penal Code).
- Section 69 should be limited in scope to information which is genuinely secret in nature.
- Section 73 should be amended to prevent its application to service providers (absent explicit and intentional involvement by them in criminal behaviour).
- Section 75 should be substantially revised to limit its application to cases where there is a real and serious threat to national security which can only be addressed through surveillance.
- The terms "emergency" and "public interest" in section 77 should be defined narrowly and clear procedural and transparency rules should be added into this provision.

6. The News Media Law

Section 9 of the 2014 News Media Law[28] is the only section in Chapter IV, which is titled "Responsibilities and Codes of Conduct to be Complied by News Media Workers". It contains a number of substantive provisions that limit the content of what may be disseminated by news media outlets. Although it does not refer explicitly to digital content, the definition of 'media' includes 'Internet Media' and most mainstream media in Myanmar do have online versions. At the same time, the scope of this Law is limited to news media (so that, for example, it does not

[28] 14 March 2014. Available at: http://www.burmalibrary.org/docs17/2014-Media_Law-en.pdf.

apply to individual social media posts). Pursuant to sections 25 and 26 of the Law, sanctions ranging from MKK 100,000 to 1,000,000 (approximately USD 73 to 730), as well as sanctions under other laws, may be imposed for breach of different parts of section 9.

Although these are relatively modest penalties, they are still sanctions and would be imposed via court processes, which would be difficult for many media in Myanmar to pay for. Better practice in this area is not to create direct standards in a media law but instead to grant the oversight body, in this case the Myanmar Press Council (MPC), created by the Law, the power to elaborate its own, more detailed, standards for the news media in a code of conduct, and then to apply them via a self-run complaints system. This would provide redress to citizens who were harmed by unprofessional media reporting, while at the same time ensuring that, overall, the system was sensitive to the working reality of the media. Section 9(i) of the Law does provide that news media should respect any standards adopted by the MPC, but the rest of the section imposes direct restrictions on content.

A number of the provisions in section 9 are unduly broad or limiting. For example, section 9(a) requires news media to ensure the accuracy and completeness of "every bit of information". As anyone who has worked as a journalist will know, this is simply not realistic. Even the very best journalists sometimes make mistakes, taking into account their duty to report in a timely fashion in the public interest. A more appropriate standard is to require media to ensure due accuracy of the news.

Section 9(c) calls on media to respect the presumption of innocence until someone has been convicted and to refrain from engaging in criticism which amounts to "contempt of court". Under international law, while expression may be restricted to protect the rights of others, including the presumption of innocence, this does not mean that media cannot report on ongoing cases or even venture an opinion as to the guilt or innocence of an accused person prior to the case being decided. It is only where this could be expected to bias the court – which should be only in the rarest of cases – that such reporting might be prohibited.

It is also important to allow the media to report freely on the activities of judges and courts given that the judiciary represents a public institution which plays a key role in a democracy and the strong public interest in holding this institution to account. In their 2002 Joint Declaration, the special international mandates on freedom of expression stated: "Special restrictions on commenting on courts and judges cannot be justified; the judiciary play a key public role and, as such, must be subject to open public scrutiny."[29] Historically, contempt of court rules have failed to strike an appropriate balance between freedom of expression and the need for open criticism of courts, on the one hand, and the need to protect the independence of the judiciary, on the other.

[29] 10 December 2002. Available at: http://www.osce.org/fom/66176.

Section 9(f) prohibits the publication of content subject to an intellectual property right without asking permission from the owner. While this is not a problematical provision *per se*, it does lack nuance. Much of the content that is protected by intellectual property may be reproduced and published by journalists without violating those intellectual property rights. For example, journalists have a right to quote from works and to engage in commentary and criticism regarding those works. This provision will probably be misunderstood by many journalists, and perhaps others, to suggest a blanket ban on reproducing any protected works.

Section 9(g) is yet another defamation provision, providing: "[W]riting style which deliberately affects the reputation of a specific person or an organization or generates negative impact to the human right shall be avoided". At one level, this can be seen as positive, inasmuch as it avoids the penalty of imprisonment for defamation that is provided for in the Penal Code and the other defamation rules described above. At the same time, it fails to provide for a proper regime for defamation, including defences and so on. This is a good example of where it would be far preferable to elaborate on the specifics in a code of conduct for the media adopted by the MPC.

Section 9(h) provides: "Ways of writing which may inflame conflicts regarding nationality religion and race shall be avoided". This provision falls within the purview of Article 20(2) of the ICCPR, which is the only provision in the ICCPR that actually requires States to prohibit certain speech, namely, "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence". Article 20(2) imposes a clear requirement of intent to incite to discrimination, hostility or violence, as well as a requirement of a close and direct causal relationship between the impugned statement and these outcomes.[30] Section 9(h) fails to require intent or a close causal relationship between the speech and the result – since it uses the term "may" to describe this relationship – and is, as a result, overly broad. This is again an area where a code of conduct approach would be far preferable.

Recommendations:

- Consideration should be given to removing all of the direct content rules from section 9 and instead providing for these to be elaborated in a code of conduct adopted by the MPC. The law could, however, indicate the types of issues that such a code would be required to address. The following recommendations represent a second-best alternative to this.
- Section 9(a) should be amended to include a qualifier, such as "due regard to accuracy" rather than imposing an absolute requirement in this regard.
- Section 9(c) should be amended to allow for free media reporting both on ongoing cases and the judiciary as an institution, except where this would really undermine the presumption of innocence or the independence and

[30] Centre For Law and Democracy and International Media Support, *Briefing Note Series: Freedom of Expression* (2014), pp. 34-5. Available at: http://www.law-democracy.org/live/wp-content/uploads/2012/08/Briefing-notes.full-version.Eng_.pdf.

authority of the judiciary.
- Section 9(f) should be amended to make it explicit that news media have the right to engage in fair use of content which is subject to intellectual property rights.
- Section 9(g) should either be repealed or amended to provide for appropriate limitations and defences to defamation.
- Section 9(h) should either be repealed or amended to reflect more closely the language of Article 20(2) of the ICCPR.

7. The Penal Code

The Penal Code contains a large number of restrictions on speech, including digital speech, that are problematical from a freedom of expression point of view. It is beyond the scope of this report to engage in an exhaustive analysis of these provisions. For current purposes, we analyse only the restrictions that relate to religion, broadly described as 'blasphemy' rules, given the importance of these rules in Myanmar at present. These rules are found in Chapter XV of the Penal Code, titled "Of Offences Relating to Religion". Two of the key provisions are as follows:

> 295A. Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of [persons dent in the Union] by words, either spoken or written, or by visible representations, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
>
> 298. Whoever, with the deliberate intention of wounding the religious feelings of any person, utters any word or makes any sound in the hearing of that person or makes any gesture in the sight of that person or places any object in the sight of that person, shall be punished~ with imprisonment of either description for a term which may be extend to one year, or with fine or with both.

The right to practise one's religion is a human right protected by Article 18 of the ICCPR. However, mere criticism of a religion, even where that is done in a way that offends or wounds the feelings of the adherents of that religion, does not, of itself, prevent anyone from practising their religion. A delicate balancing regarding speech which relates to religious matters is necessary to ensure respect for both the right to freedom of expression and the right to religion. Under international law, only speech which meets the conditions of Article 20(2) of the ICCPR, prohibiting hate speech, may be prohibited to protect religions. This focuses on protecting individual adherents to a religion, rather than the religion *per se*, as a belief structure or set of ideas.

As a result, blasphemy laws which go beyond prohibiting incitement to discrimination, hostility or violence against adherents to a particular religion and which limit speech which merely denigrates or insults that religion's beliefs or

symbols, are not regarded as legitimate.[31] Reflecting this, the 2011 General Comment by the UN Human Rights Committee states:

> Prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant, except in the specific circumstances envisaged in article 20, paragraph 2, of the Covenant.[32]

The rules in the Penal Code on Offences Relating to Religion, including the two provisions cited above, fail to conform to these standards. They protect feelings as opposed to protecting individuals against discrimination, violence or hatred. In addition, they protect religious beliefs, as such, as opposed to the people who hold those beliefs.

Recommendation:

- Chapter XV of the Penal Code should be revised to bring it into line with the standards noted above, in particular so that it only limits speech to protect religious believers against discrimination, violence and hatred. In particular, sections 295A and 298 should be repealed.

8. Conclusion

Developing a legislative framework to regulate online speech is a tricky and delicate endeavour that is only rendered more challenging by the complexity, technical sophistication and rapidly evolving nature of digital technologies. These challenges mean that legislative drafting and reform efforts need to be sure to engage with civil society and to make sure that the concerns of all stakeholders are taken into account in order to avoid clumsy or technically ineffective rules, as well as laws which prohibit innocuous or benign digital behaviours alongside harmful ones.

Engagement with legal and technical experts who possess the expertise and skill sets that lawmakers often lack, or who may offer insights and perspectives that are otherwise absent, is therefore of paramount importance. A range of civil society players in Myanmar, including the legal organisation, Myanmar Media Lawyers' Network (MMLN), can play a key role in this regard by helping to ensure that laws limiting digital content respect international and constitutional guarantees of freedom of expression.

This report highlights some of the more problematical provisions in various Myanmar laws, including the Electronic Transactions Law, Official Secrets Act, Telecommunications Law, News Media Law and Penal Code. It is now up to policy makers and the Myanmar authorities to ensure that these laws are

[31] Centre For Law and Democracy and International Media Support, *Briefing Note Series: Freedom of Expression* (2014), p. 36. Available at: http://www.law-democracy.org/live/wp-content/uploads/2012/08/Briefing-notes.full-version.Eng_.pdf.
[32] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 48.

amended so that they strike an appropriate balance between freedom of expression and the various interests they purport to protect.