



CENTRE FOR LAW
AND DEMOCRACY

Philippines

Analysis of the Cybercrime Prevention Act of 2012

November 2012

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction

On 12 September 2012, Philippine President Benigno Simeon C. Aquino III signed into law Republic Act No. 10175 (the Cybercrime Prevention Act).¹ Although the law's stated purpose is to facilitate the prevention, detection, investigation and prosecution of criminal acts online, and the law's proponents claim that it effectively serves to extend the Philippines' constitutional protections into the digital realm,² it has been criticised by journalists and civil society organisations who claim that it violates freedom of expression. In the days following its passage, fifteen separate petitions were filed in the High Court challenging fourteen of the law's provisions.³ As a result, the Supreme Court has suspended implementation of the Cybercrime Prevention Act for 120 days, in order to allow the challenges to proceed.

The emergence of the online world has created enormous opportunities, in terms of economic growth and due to the Internet's expanding role as a vital delivery mechanism for human rights, particularly freedom of expression.⁴ By the same token, it has given rise to a range of challenges from a legal and regulatory perspective. Governments seeking to regulate the Internet need to find an appropriate balance between addressing legitimate security and other legal concerns, and respecting freedom of expression online and safeguarding the qualities of the Internet that make it such a valuable medium. An overly heavy-handed approach to online regulation can breach human rights and threaten the Internet's usefulness and character, both domestically and internationally.

This Analysis considers the Cybercrime Prevention Act from the perspective of international guarantees of freedom of expression. It discusses the major areas where this law violates international human rights standards, and makes recommendations as to how to avoid these problems while still delivering the desired benefits.

1. Key Freedom of Expression Standards

¹ Available at: <http://www.gov.ph/2012/09/12/republic-act-no-10175/>.

² Marvin Sy, "Give Cybercrime Prevention Act a chance", *The Philippine Star*, 23 September 2012. Available at:

<http://www.philstar.com/Article.aspx?articleId=851856&publicationSubCategoryId=63>.

³ Tetch Torres, "SC issues TRO vs cyber law", *Inquirer News*, 9 October 2012. Available at: <http://newsinfo.inquirer.net/285848/sc-stops-cyber-law>.

⁴ For a broader discussion of the Internet and human rights see: 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:

<http://www.law-democracy.org/wp-content/uploads/2010/07/final-Internet.pdf>.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

Freedom of expression is recognised as a fundamental human right. It is protected under Article 19 of the *Universal Declaration of Human Rights* (UDHR),⁵ a UN General Assembly resolution, which states:

Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers.

Freedom of expression is also protected in Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR),⁶ which the Philippines ratified in October 1986:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
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 or reputations of others;
 - (b) For the protection of national security or of public order (ordre public), or of public health or morals.

This imposes a strict three-part test for restrictions. In its most recent General Comment on Article 19 of the ICCPR, adopted in September 2009, the UN Human Rights Committee stated:

Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be “provided by law”; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality. [references omitted]⁷

First, the restriction must be provided by law or imposed in conformity with the law. This implies not only that the restriction is based on a legal provision, but also that the law meets certain standards of clarity and accessibility. Where restrictions are vaguely drafted, they may be interpreted in a way that gives them a range of different meanings. This gives the authorities the discretion to apply them in situations which bear no relation to the original purpose of the law or to the legitimate aim sought to be protected. For those subject to the law, vague provisions fail to give adequate notice of exactly what conduct is prohibited. As a result, they exert an unacceptable chilling effect on freedom of expression as individuals steer

⁵ UN General Assembly Resolution 217A(III) of 10 December 1948.

⁶ UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.

⁷ General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 22. See also *Mukong v. Cameroon*, 21 July 1994, Communication No.458/1991, para.9.7 (UN Human Rights Committee).

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

well clear of the potential zone of application to avoid censure. As the Human Rights Committee has stated:

For the purposes of paragraph 3, a norm, to be characterized as a “law”, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.⁸

Second, the restriction must pursue one of the legitimate aims listed in Article 19(3). It is quite clear from both the wording of the article and the views of the UN Human Rights Committee that this list is exclusive and that restrictions which do not serve one of the legitimate aims listed are not valid:

Restrictions are not allowed on grounds not specified in paragraph 3, even if such grounds would justify restrictions to other rights protected in the Covenant. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated. [references omitted]⁹

It is not sufficient, to satisfy this part of the test, for restrictions on freedom of expression to have a merely incidental effect on one of the legitimate aims listed. The measure in question must be primarily directed at that aim.¹⁰

Third, the restriction must be necessary to secure the aim. The necessity element of the test presents a high standard to be overcome by the State seeking to justify the interference, apparent from the following quotation, cited repeatedly by the European Court:

Freedom of expression, as enshrined in Article 10, is subject to a number of exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established.¹¹

Courts have identified three aspects of this part of the test. First, restrictions must be rationally connected to the objective they seek to promote, in the sense that they are carefully designed to achieve that objective and that they are not arbitrary or unfair. Second, restrictions must impair the right as little as possible (breach of this condition is sometimes referred to as ‘overbreadth’). Third, restrictions must be

⁸ General Comment No. 34, *ibid.*, para. 25.

⁹ *Ibid.*, para. 22. See also *Mukong v. Cameroon*, note 7, para.9.7.

¹⁰ As the Indian Supreme Court has noted: “So long as the possibility [of a restriction] being applied for purposes not sanctioned by the Constitution cannot be ruled out, it must be held to be wholly unconstitutional and void.” *Thappar v. State of Madras*, [1950] SCR 594, p. 603.

¹¹ See, for example, *Thorgeir Thorgeirson v. Iceland*, 25 June 1992, Application no. 13778/88, para. 63.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

proportionate to the legitimate aim. The proportionality part of the test involves comparing two factors, namely the likely effect of the restriction on freedom of expression and its impact on the legitimate aim which is sought to be protected.

The UN Human Rights Committee has summarised these conditions as follows:

Restrictions must not be overbroad. The Committee observed in general comment No. 27 that “restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law”. The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.

When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat. [references omitted]¹²

The right to freedom of expression also finds protection in the Bill of Rights of the Constitution of the Philippines:¹³

Article III

...

Section 4:

No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.

Given that the Philippines has ratified the ICCPR, the Constitution of the Philippines should, to the extent reasonably possible, be interpreted in a manner that gives effect to the country's obligations under the ICCPR. In other words, restrictions on freedom of expression in the Philippines should receive constitutional assessment that is at least as protective as the three-part test under international law.

As a medium of communication, it is evident that any regulation of the Internet must conform to freedom of expression standards. The four special international mandates on freedom of expression – the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-

¹² General Comment No. 34, note 7, paras. 34 and 35.

¹³ Available at: <http://www.gov.ph/the-philippine-constitutions/the-1987-constitution-of-the-republic-of-the-philippines/the-1987-constitution-of-the-republic-of-the-philippines-article-iii/>.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

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 – have adopted a Joint Declaration on a freedom of expression theme since 1999. The 2011 Joint Declaration, on Freedom of Expression and the Internet, included the following statement:

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).¹⁴

Thus, in order to be legitimate, the restrictions in the Cybercrime Prevention Act should be consistent with the, ICCPR, and in particular they should be justifiable under the three-part test.

2. Criminal Content Prohibitions

General Extension of Criminal Offences

A particular concern with the Cybercrime Prevention Act is section 6, which appears to extend liability for all crimes, including those involving content offences, to the online world, while also increasing the penalties for these crimes:

All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

The rationale underlying this provision is puzzling. Most obviously, it is difficult to understand why legislators should feel the need to treat crimes more seriously if they are committed online. Indeed, if anything, the opposite should be true, at least for crimes involving content. As Principle 1 of the Council of Europe's the Declaration on freedom of communication on the Internet states:

Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.¹⁵

¹⁴ Adopted 1 June 2011, clause 1(a). Available at: <http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf>.

¹⁵ Adopted by the Committee of Ministers of the Council of Europe on 28 May 2003.

Less obvious, but perhaps even more serious, is the failure of this provision to take into account the particular features of online communication. The 2011 Joint Declaration on Freedom of Expression and the Internet included the following statement:

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.¹⁶

The specific nature of the Internet, and in particular its ability to foster open, participatory debate, needs to be taken into account when applying content restrictions designed for an offline world to it. The rigidity of the approach taken in section 6 may be contrasted with the flexibility of a case-by-case approach, which is essentially available currently. Under this approach, online content that potentially breaches criminal law provisions could, as appropriate, be challenged in court, where interpretation would allow for any necessary adaptations to protect freedom of expression online.

This general problem is exacerbated by section 5(a) of the Cybercrime Prevention Act, which criminalises wilfully aiding or abetting in the commission of any offence under the Act. Depending on how “wilfully” is defined, this could mean that Facebook and Twitter themselves incur liability for any dissemination of illegal statements by their users, since designing and maintaining the platform upon which an illegal statement is published could be understood as aiding and abetting in its publication. These broad extensions of liability are completely incongruous with the fluidity of online speech. It would be impossible for Facebook or Google to function if they were to be held responsible for every statement that is made through their services. As such, provisions like this pose a real threat to the functionality of the Internet.

Another problem with the Cybercrime Prevention Act is the fact that section 7 allows for different charges to be levied as a result of a single publication:

Liability under Other Laws. — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

Given that many publications put out the same material online and offline, this provision could allow multiple criminal charges to be laid over the same statement. In other words, a user publishing an article in a magazine that appears both in print and online could be charged twice.

¹⁶ Note 14, clause 1(c). See also *Reno v. ACLU*, 521 US 844 (1997), in which the United States Supreme Court held that forms of regulation designed for other mediums could not just be applied to the Internet.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

The 'Crime' of Defamation

These problems are particularly concerning in relation to defamation. In line with the need for restrictions on freedom of expression to be constructed as narrowly as possible, libel should be considered solely as a civil, rather than a criminal matter. Under no circumstances is it justifiable to impose custodial sentences for defamation, because such oppressive sanctions are simply not necessary to ensure that the reputations of people are adequately protected. According to a General Comment issued in September 2011 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.¹⁷

Defamation is essentially a dispute between two private individuals and, if a person believes that their reputation has been harmed, the civil law can provide an adequate remedy for this. 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 decriminalisation or the relaxing of penalties have 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.

In the Philippines, defamation remains a criminal offence pursuant to Articles 353-355 of the Revised Penal Code. The UN Human Rights Committee has already held in one case that the application of criminal defamation in the Philippines represents a breach of the right to freedom of expression as protected by Article 19 of the ICCPR.¹⁸ Rather than moving away from criminal defamation, section 4(c)(4) of the Cybercrime Prevention Act specifically extends the criminal defamation provisions in Article 355 of the Revised Penal Code not only into the online realm, but also into “any other similar means which may be devised in the future”.

Since the Cybercrime Prevention Act does not specifically provide for a penalty for section 4(c)(4), the provisions of section 6 would apply, so that defamatory statements published online are now punishable by up to 12 years imprisonment. Considering that Philippine law already punishes defamation far more harshly than international human rights standards permit, this shift is extremely problematical.

¹⁷ General Comment No. 34, note 7, para. 47.

¹⁸ *Adonis v. the Philippines*, 26 October 2011, Communication No. 1815/2008, para. 8.10.

The Cybercrime Prevention Act is also problematic in that it fails to provide for any safe harbour provision for innocent disseminators of defamatory statements. Article 354 of the Revised Penal Code states:

Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown, except in the following cases

1. A private communication made by any person to another in the performance of any legal, moral or social duty; and
2. A fair and true report, made in good faith, without any comments or remarks, of any judicial, legislative or other official proceedings which are not of confidential nature, or of any statement, report or speech delivered in said proceedings, or of any other act performed by public officers in the exercise of their functions.

This is highly problematical in any context. Given that these provisions represent a restriction on a fundamental human right, freedom of expression, the presumption about malice should run the other way (i.e. the onus should lie on the plaintiff to prove malice), and there should be absolute protection for true statements, on the basis that one cannot defend a reputation that one does not deserve.

They are even more problematical in the online context, where publication and republication are far more fluid concepts and the discourse is understood to be more freewheeling. Liability may now attach to any Twitter user who retweets a defamatory statement, or a blogger who reposts a defamatory statement found elsewhere. For that matter, search engines such as Google could be held liable for returning search results containing a defamatory statement. As far-fetched as this might seem, it is unfortunately not without precedent. A woman in India was recently arrested for clicking 'like' on a Facebook posting.¹⁹

In order to live up to its international human rights obligations, the Philippine government should not only remove these problematic provisions within the Cybercrime Prevention Act, but they should completely repeal their criminal defamation laws.

Recommendations:

- Section 6 of the Cybercrime Prevention Act should be deleted.
- The standards under section 5(a) of the Cybercrime Prevention Act should be amended to replace the notion of wilful with a requirement of intentionally aiding or abetting the commission of an offence.
- Section 7 of the Cybercrime Prevention Act should be amended to eliminate the possibility of multiple charges being filed for the same statement.
- Section 4(c)(4) of the Cybercrime Prevention Act and Articles 353-355 of the

¹⁹ See <http://www.csmonitor.com/World/Asia-South-Central/2012/1119/Woman-hits-like-on-Facebook-gets-arrested-in-India>.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

Revised Penal Code should be deleted.

3. Removal of Websites

A significant problem with the Cybercrime Prevention Act is that it grants the Department of Justice sweeping power to censor websites. Section 19 states:

Restricting or Blocking Access to Computer Data. — When a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

Such a restriction or blocking order is a form of prior censorship. Although this is not entirely ruled out under international law, international courts have held that such measures must be treated with the greatest suspicion. The European Court of Human Rights, for example, has stated:

[T]he Court has emphasised that while Article 10 [which guarantees freedom of expression] does not prohibit the imposition of prior restraints on publication, the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court.²⁰

The special international mandates have made it clear that mandatory blocking of websites (as opposed to user blocking based on personal preferences) is extremely problematical, noting in their 2011 Joint Declaration:

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

Although it is not stated explicitly in the quotation above, it flows from that statement that such blocking could only ever be justifiable in the context of judicial action. The fact that section 19 gives a political organ of government, the Department of Justice, the power to unilaterally block websites based on a *prima facie* finding, with no judicial involvement, simply cannot be justified as a restriction on freedom of expression.

It is not just that this power might be abused for political purposes, although that is serious enough. It is also that allowing, indeed requiring (for the provision uses the term ‘shall’), a minister to wield such power effectively deprives those responsible

²⁰ *Mosley v. the United Kingdom*, 10 May 2011, Application no. 48009/08, para. 117.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

for the website of any due process protection. In many cases, the issue will be complex. For example, whether a statement is or is not defamatory can be legally and factually complicated and highly contextual, and is normally something that should be dealt with by a court. Standards for what constitutes pornography or obscenity are even more vague and subjective, and there may also be political pressure to remove material of this nature, making this another area where section 19 is ripe for abuse, taking into account section 4(c)(1) of the Cybercrime Prevention Act, which criminalises sexual content online.

Even where it is reasonable to require a website containing defamatory or other illegal material to remove this material after a judicial decision is handed down on the merits of the case, interim blocking of material could only be acceptable where any delay in removing it would cause irreparable and serious harm, necessitating immediate action. Even in this case, it should be necessary to obtain the approval of a judge for the blocking action, if necessary on an urgent basis.

Section 19 of the Cybercrime Prevention Act is also problematical inasmuch as blocking of a website represents an extreme sanction, analogous, as noted in the statement of the special international mandates to banning a newspaper, which would rarely if ever be justified. Yet in many cases, the only practical way to block access to material would be to block the whole website. For example, posts on social platforms such as Facebook and Twitter are often distributed throughout a diverse network of user pages, making it functionally difficult to selectively block out the areas of the network that contain a particular statement. In other words, enforcement of section 19 could mean that the posting of an illegal statement on Facebook, Twitter or YouTube would require the Minister of Justice to block these services entirely, although in the vast majority of cases more limited measures, such as requiring the owner of the website to take down offensive material or face the normal sanctions for refusing to obey a court order, would suffice.

Recommendation:

- Section 19 should be deleted.

4. Universal Jurisdiction

The Internet transcends national borders and is ill suited to traditional understandings of territoriality. This problem was addressed 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

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

OSCE Representative on Freedom of the Media, and the OAS Special Rapporteur on Freedom of Expression – which included a focus 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.²¹

However, section 21 does not follow this principle, and instead provides for incredibly broad jurisdiction under the Cybercrime Prevention Act:

Jurisdiction. — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act. including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

Anything published on the Internet is, generally speaking, available everywhere in the world through the use of local servers and computers or mobile devices. As a result, the phrasing of this provision is such that a vast range of illegal material published anywhere could be subject to prosecution under this law.

For example, imagine a French citizen in France who writes a blog post which under Philippine law is defamatory of another French citizen. Because the statement was made online, it will be accessible in the Philippines through the use of local computer systems. If even one person who happens to be in the Philippines while the material is still online and who happens to know of the French citizen who was defamed views the material, it would be subject to the blocking and defamation provisions of the Cybercrime Prevention Act. The same would be true if the defamed French citizen should ever visit the Philippines while the material was still available online. In effect, this provision gives Philippine authorities the mandate and responsibility to police the entire Internet, and to interpose themselves in cases that have no connection whatsoever to the Philippines.

Claims of universal jurisdiction over the Internet present a significant challenge to freedom of expression online because they subject users to a patchwork of conflicting legal frameworks. This depresses online speech by forcing websites to either regulate all of their content consistent with the world's harshest and most restrictive standards – a lowest common denominator approach – or to block the availability of their content in jurisdictions whose laws they do not wish to conform

²¹ Adopted 21 December 2005. Available at: <http://www.osce.org/fom/27455>.

to. This, in turn, threatens to effect a balkanisation of the Internet, undermining its power as a global medium.

Overly broad assertions of jurisdiction have proven to be particularly problematic in the context of defamation, where they have led to the phenomenon of “libel tourism”, whereby well-resourced litigants file suit in countries with plaintiff friendly defamation laws. The most notorious destination for libel tourism, the United Kingdom, is currently in the process of amending its laws, in part to prevent this type of abuse.

It is unreasonable for the government of the Philippines to expect to regulate the entire Internet. Instead, the jurisdiction of the Cybercrime Prevention Act should be limited to cases where either the offending conduct originates within the Philippines or where substantial harm has taken place within the Philippines.

Recommendation:

- Section 21 should be amended so that it only applies to acts committed within the Philippines or to acts where substantial harm takes place in the Philippines.

5. Sexual Offences

Section 4(c)(1) of the Cybercrime Prevention Act, which criminalises cybersex, should be reconsidered:

Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

It is to be expected that different countries will have different attitudes towards pornography and obscenity. As the UN Human Rights Committee has pointed out, “public morals differ widely. There is no universally applicable common standard. Consequently, in this respect, a certain margin of discretion must be accorded to the responsible national authorities.”²²

However, while the Philippines would not be the first country in the world to take such a firm a stand against sexual content on the Internet, this approach is considerably harsher than that found in most democratic countries. It also goes far beyond the Act’s stated purpose of protecting children from exploitation by

²² *Hertzberg et al. v. Finland*, 2 April 1982, Communication No. 61/1979, para. 10.3.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

criminalising any sexual content at all, including activity that takes place between consenting adults.

In line with the three-part test, the Philippine government should question whether it is actually necessary to criminalise and block all sexual content online. Fully enforcing this law would be a massive undertaking which would require enormous resources dedicated to locating and blocking offending websites. It therefore merits careful consideration as to whether the government of the Philippines actually intends to assume such a broad responsibility.

Recommendation:

- Section 4(c)(1) should be reconsidered in light of its broad applicability and the resources necessary to enforce it.

6. The “Reckless” Standard

As the country where the notorious ILOVEYOU virus, one of the world’s first major online security scares, originated, there is an understandable sensitivity within the Philippines over the need to contain computer viruses. Nonetheless, section 4(a)(3) of the Cybercrime Prevention Act goes troublingly far in its attempt to combat the spread of malicious code:

Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

While it is certainly reasonable to criminalise the intentional introduction or transmission of computer viruses, the use of the “reckless” standard is problematic. Levels of technical sophistication vary dramatically between different users. This is particularly true as the Internet spreads into communities with limited levels of education and computer literacy. In this context, it bears questioning as to how one determines the level of technical understanding necessary for a person to be using the Internet responsibly (i.e. not recklessly)?

It could be argued that any PC user who surfs the Internet without anti-virus software, or even who fails to regularly update their anti-virus software, is being reckless. What about someone who forwards on an email after their anti-virus software has flashed up a warning? While this may not be behaviour one might wish to encourage, it is unfortunately common among computer users, and hardly justifies a criminal sanction.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

More generally, criminalising behaviour which falls short of manifesting full mental responsibility, such as criminal negligence, is always controversial. While such rules are accepted in some areas, such as the operation of automobiles, this is hardly analogous to using a computer. Other, more positive approaches, such as education and awareness raising, are a more appropriate way to address this problem.

Recommendation:

- Section 4(a)(3) should be amended to remove the word “reckless”.

7. Cybersquatting

Cybersquatting, where an individual acquires a particular domain name in bad faith in order to sell it on to a company or user with an interest in it, is a common phenomenon around the world. However, it is a problem that can be easily managed through civil or administrative procedures that allow aggrieved parties an opportunity to wrest control of domain names that are being held in bad faith. Given that most countries have established effective civil mechanisms to deal with this problem, it is difficult to understand why Section 4(a)(6) of the Cybercrime Prevention Act criminalises it:

Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

- (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- (iii) Acquired without right or with intellectual property interests in it.

The fact that most countries treat cybersquatting as a civil matter, and deal with it effectively as such, means that Section 4(a)(6) could not pass muster under the necessity part of the three-part test for restrictions on freedom of expression.

It is even more troubling that this prohibition is not limited to cybersquatting as commonly understood, as described above. Instead, the law extends to any domain name which is “similar” to an existing trademark or name, and can extend to domain names registered for the purpose of “destroying reputation”, even though this practice can be perfectly legitimate as protected speech.

For example, the People for Ethical Treatment of Animals, a prominent animal-rights organisation in the United States, launched a campaign against fast-food

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

restaurant Burger King's use of factory-farmed meats that featured the website www.MurderKing.com. The website, being phonetically similar to Burger King's trademarked name and being designed to attack the company's reputation, would likely be illegal under the Cybercrime Prevention Act, even though it is clearly legitimate political speech as a critique of the fast food restaurant's approach to animal welfare. Similarly, websites such as whynotobama.com, aimed at defeating the United States President in the last election, would also probably fall foul of this provision given that they incorporate the candidate's name.

Ultimately, this provision is both unnecessary and overly damaging to freedom of expression. It should be deleted, and legitimate cases of cybersquatting should be dealt with as civil matters.

Recommendation:

- Section 4(a)(6) should be deleted.

8. Data Retention and Monitoring

The Cybercrime Prevention Act includes significant new measures for surveillance of the Internet. Section 12 authorises law enforcement authorities to monitor online traffic data with due cause but without the need for a warrant. The law defines traffic data as including information about a communication's origin, destination and duration, but not its content or the identity of the parties. Service providers are compelled to assist law enforcement in gathering this information.

Section 13 requires service providers to build a database of information about their subscribers, including by recording all traffic and content information and the identity behind each IP address, and to preserve this information for at least six months, and for an additional six months upon the specific request of law enforcement officials.

The Philippines is not alone in enacting these types of surveillance measures. Similar procedures have been drafted elsewhere, most notably in the European Union, where such legislation is meant to be harmonised through the Data Retention Directive.²³ However, these laws have also been subject to significant criticism, and have been overturned in Germany, Romania and the Czech Republic. The Data Retention Directive itself is also the subject of an ongoing challenge before the Court

²³ Directive 2006/24/EC.

of Justice of the European Union due to its problematic impact on privacy and freedom of expression.²⁴

The problem with mandatory, generalised data retention rules, from the perspective of freedom of expression, is that user privacy is a critical component to safeguarding online speech. The freewheeling nature of online debate is significantly enhanced by the feeling of anonymity enjoyed by users. As a result, moves to enhance surveillance of the web can chill online speech by reducing their sense of security and anonymity. Indeed, data retention and surveillance mechanisms have the potential to turn the Internet from a medium where users are comparatively free and anonymous to one where their actions are subject to far greater scrutiny than elsewhere. A person walking down the street can pick up pamphlets or newspapers, or make comments to bystanders, without having these actions tracked and recorded. But on the Internet, every move that a user makes, every comment they put out and every article they read leaves a digital trail which, as a result of data retention initiatives, would be tracked and archived.

The Cybercrime Prevention Act is particularly troubling in this regard because of the scope of surveillance that law enforcement authorities are allowed to carry out without a warrant. Section 12, which allows police to monitor communications based on their origins and endpoints, appear to allow unrestricted data gathering about the activities of a particular IP address. The only thing that would require a warrant would be confirmation of the identity of the user behind the IP address.

The problem with this approach is that individual users can often be identified from IP addresses. Online sleuthing will often enable investigators to trace an IP address back to a specific location or individual even if that information is not specifically provided. In 2011 the European Court of Justice cited this rationale in their finding that IP addresses are protected as personally identifiable data.²⁵ In other words, a technically sophisticated investigator will be able to determine the identity of the user behind the IP address, even without the warrant this is supposed to require, which means that, practically speaking, the Cybercrime Prevention Act allows for almost unlimited surveillance. This is a sure recipe for chilling online speech.

These rules are also problematic inasmuch as they require ISPs to create and store enormous amounts of data about their users. Similar provisions elsewhere have been criticised due to questions about the ability of ISPs to safeguard this information. These databases will contain enormous quantities of personal information, making them a tempting target for hackers. This was demonstrated in

²⁴ See <http://register.consilium.europa.eu/pdf/en/12/st12/st12785.en12.pdf>.

²⁵ *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL*, ECJ, No. C-70/10, 11/24/11. Available at: <http://www.teutas.it/giurisprudenza/corte-di-giustizia-europea/849-ecj-scarlet-extended-sa-v-societe-belge-des-auteurs-compositeurs-et-editeurs-scrl-sabam-c-7010.html>.

July 2012, when the hacker collective Anonymous responded to proposals to require Australian ISPs to store two years worth of user information by promptly hacking into the database of a major ISP.²⁶

Data retention provisions such as those found in Sections 12 and 13 of the Cybercrime Prevention Act have met with significant criticism around the world. For example, similar frameworks have been criticised by the European Data Protection Supervisor and staunchly opposed by the Electronic Frontiers Foundation.²⁷ Although the emergence of the online world has given rise to new challenges for law enforcement officials, these challenges can be adequately addressed without compromising user privacy and anonymity, which in turn threaten to severely chill online speech.

Recommendations:

- Section 12 should erect more significant procedural barriers to official monitoring of Internet activity, which are analogous to the systems for protection of the confidentiality of offline forms of communication. At a minimum, law enforcement officials should be required to obtain a warrant in order to requisition data about a particular IP address.
- Section 13 should be deleted.

²⁶ Joel Falconer, "Anonymous hacks Australian ISP AAPT to demonstrate data retention problems", The Next Web, 26 July 2012. Available at: <http://thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/>.

²⁷ See <http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf> and <https://www.eff.org/issues/mandatory-data-retention>.

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy