

Should Hong Kong Legislate on Cyberbullying? If so, how?

1 Introduction

Cyberbullying is on the rise, and our government has been preaching self-help. This paper argues that Hong Kong should have specific legislation to deal with the issue of cyberbullying, and will make some suggestions as to how this task should be approached.

We will begin with an overview of the phenomenon of cyberbullying. Some real cases will be referred to in an attempt to demonstrate that cyberbullying is capable of causing serious harm, which is more than sufficient justification for legislative intervention. We will then turn our attention to the current legal landscape, both local and overseas.

After that, we will examine some arguments against legislating on the subject of cyberbullying, and I will explain why we should nevertheless press for legislation. Next, we will discuss what the statute should cover, what its aims should be, and so on.

2 Overview

2.1 What is cyberbullying?

Many would agree with me that cyberbullying is easier to describe than to define. While “[k]ids usually know it when they see it”,¹ different jurisdictions and organisations often adopt different definitions. Some definitions require that the acts be “committed by minors and directed at other minors”,² while some define cyberbullying as “involving the use of information and communication technologies to support deliberate,

¹ http://stopcyberbullying.org/what_is_cyberbullying_exactly.html Retrieved Feb 21, 2015.

² See the definition in the *Encyclopedia Britannica Online*, “stalking (crime)”. Retrieved Feb 15, 2015.

repeated, and hostile behavior by an individual or a group that is intended to harm others”.³

Looking at examples often assists in understanding. The Australian Human Rights Commission has helpfully given a list of examples as to what forms cyberbullying may take, which are truly reminiscent of life in high school. Those examples include: being sent mean or hurtful text messages from someone you know or even someone you don't know; people spreading rumours about you via emails or social networking sites or text messages; people setting up fake profiles pretending to be you, or posting messages or status updates from your accounts.⁴

While there is every reason to believe that these forms of cyberbullying still exist, it seems that a new form has evolved over recent years. In modern day Hong Kong, the most conspicuous form of cyberbullying seems to follow this pattern: a person (“the offender”) behaves in a public place in a way which another person finds offensive; that other person then takes a photo or video of the offender, uploads it to the Internet and pillories him (often in online forums). Then there comes a crowd of “netizens” shouting abuse, “sharing” the photo or video in question, digging up personal information about the offender, and so on. It looks as if a show trial is conducted on the Internet, often resulting in the offender making public apologies and begging for mercy. It is submitted that “cyberbullying” should not be given an unduly narrow definition, and should include such abusive conduct. The following discussion will proceed on the assumption that such conduct is indeed within the meaning of “cyberbullying”.

The issue of definition will be further addressed below.

2.2 Potential damage serious

It is beyond the scope of this paper to examine in great detail what damage cyberbullying can do to its victims; however, some background information will be necessary to show why it is so important to have a law

³ Bill Belsey's definition as cited in a 2010 study by the HKFYG. See introductory page at <http://yrc.hkfyg.org.hk/news.aspx?id=ba972e77-cfa2-4d64-9598-6ec3bb4a780d&corpname=yrc&i=2527> Retrieved Feb 17, 2015.

⁴ <https://www.humanrights.gov.au/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying-fact-sheet> Retrieved Feb 21, 2015.

dealing specifically with cyberbullying. For illustrative purposes, this section will refer to some real cases which have been reported in the news.

Cyberbullying can lead to loss of employment, as an article in the New York Times Magazine can powerfully demonstrate.⁵ Lindsey Stone “posed for a photograph while mocking a sign at Arlington National Cemetery’s Tomb of the Unknowns”. The photo became publicly available, and a “Fire Lindsey Stone” Facebook page was created, which was said to be “wildly popular”. Justine Sacco made a bad joke about AIDS on Twitter, which aroused the wrath of the crowd. Similarly, she lost her job. The author of the article also made the following observations: “The people I met were mostly unemployed, fired for their transgressions, and they seemed broken somehow — deeply confused and traumatized.” “It almost felt as if shamings were now happening for their own sake, as if they were following a script.”⁶

Occasionally, cyberbullying campaigns do backfire, and the result can be remarkably dramatic. It appears from the article referred to above that an Adria Richards overheard a joke which she considered to be offensive; she immediately took a photo of the man who made that joke and posted it on her Twitter account. It seems that the man got fired two days later as a result. The story did not end there: his sympathisers launched a cyberbullying campaign against Richards, who in the end also got fired.

Perhaps a bit surprisingly, victims of cyberbullying may even find it difficult to start a romantic relationship, “because we Google everyone we might date.”⁷

In the worst cases, victims of cyberbullying may even commit suicide, as in the case of Hannah Smith, a girl aged 14 from Leicestershire.⁸

Of course, in certain cases it could be argued that one cannot conclusively establish a causal link between cyberbullying and the harm done eventually. However, it is submitted that when taken as a whole, the existing state of affairs is such that it calls for action. Even if we do not

⁵ http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=1
Retrieved Feb 21, 2015.

⁶ See note 5 above.

⁷ See note 5 above.

⁸ <http://www.theguardian.com/society/2013/aug/06/hannah-smith-online-bullying> Retrieved Feb 21, 2015.

already have such cases where a causal link can be proven beyond reasonable doubt, it would indeed be tragic if we were to wait until we actually see such a case here in Hong Kong.

2.3 Cyberbullying in Hong Kong: how bad is it?

The Hong Kong Federation of Youth Groups conducted a study in 2010 on cyberbullying among Hong Kong secondary students, and the results are rather worrying.⁹ 899 out of 2978 students (i.e. 30%) said they had been cyberbullied in the previous year, and social media such as Facebook and Twitter was involved in over 50% of the cases. Of those 899 students, over 20% reported having lower self-esteem as a result. At the same time, 656 out of 2977 students (i.e. over 20%) said that they had cyberbullied others in the previous year.

In fact, cyberbullying is not new to Hong Kong – some notable cases date back to 2009.¹⁰ In 2012, one Legislative Council member noted that “incidents of cyber-bullying happen in Hong Kong from time to time.”¹¹

More recently, in October last year, the Occupy Central campaign prompted more cases of cyberbullying. It was reported that police officers and their families had been subjected to online harassment.¹² Personal attacks were made on social media; photos and personal information were gathered and uploaded. In January this year, the Office of the Privacy Commissioner for Personal Data (“the Privacy Office”) released some statistics for 2014. A total of 34 complaints were made to the Privacy Office with respect to cyberbullying, 28 of which were related to the Occupy Central movement. It must be noted that between 2013 and 2014, there had been a “five-fold increase in the number of cyberbullying cases.”¹³

⁹ http://yrc.hkfyg.org.hk/files/yrc/yrc_vs44.pdf Retrieved Feb 20, 2015.

¹⁰ See note 9 above, pp 16-17.

¹¹ <http://www.info.gov.hk/gia/general/201212/19/P201212190360.htm> Retrieved Feb 17, 2015.

¹² <http://www.scmp.com/news/hong-kong/article/1622424/arrest-over-online-harassment-police-officers-daughter> Retrieved Feb 17, 2015

¹³ http://rthk.hk/rthk/news/englishnews/20150127/news_20150127_56_1072414.htm Retrieved Feb 17, 2015.

2.4 Hong Kong: the current legal landscape

At this moment, Hong Kong has no statute law which specifically governs the issue of cyberbullying.¹⁴ Existing criminal and civil law may sometimes apply to a given case. If the bullying involves sending threats to the victim, it could amount to criminal intimidation, contrary to section 24 of the Crimes Ordinance (Cap. 200). The offence created under section 161 of the same Ordinance, “access to computer with criminal or dishonest intent”, may also be relevant. As to civil law, since the case of *Lau Tat Wai* in 2013, Hong Kong law has recognised the tort of harassment.¹⁵ While this tort has huge potential relevance in cyberbullying cases, it is not clear how the case law will develop;¹⁶ its utility to victims of cyberbullying remains uncertain.

With respect to the existing criminal law in Hong Kong, Bharwaney and Marwah in a 2013 article stated that:

“Unfortunately, pre-Internet laws are sometimes inadequate in dealing with these new forms of harassment and bullying. Much of the relevant criminal legislation is outdated and inadequate and technical developments require specially trained enforcement units.”¹⁷

Further, in January this year the Privacy Commissioner Allan Chiang Yam-wang said that cases of cyberbullying did not always “fit squarely within the bounds of the Personal Data (Privacy) Ordinance.”¹⁸

Sadly, even though the present situation is highly unsatisfactory, the SAR Government has not been very enthusiastic about changing it. In December 2012, the Government clarified its position in relation to bullying acts that are not currently criminal offences. It said that it would be “more appropriate to promote security awareness among the public and educate them on how to protect themselves when using the Internet.”¹⁹ It also said that it had launched three pilot outreaching projects with non-governmental organisations.

¹⁴ See note 11 above.

¹⁵ http://www.onc.hk/pages/show_pub.asp?pub_sid=29&pid=7878&article=update&category=civil Retrieved Feb 20, 2015.

¹⁶ See note 15 above.

¹⁷ Mohan Bharwaney and Azan Marwah, “Personal Data Privacy in the Digital Age”, 43 HKLJ 801, at 830.

¹⁸ <http://www.scmp.com/news/hong-kong/article/1693585/occupy-central-protests-blamed-increase-cyberbullying-hong-kong> Retrieved Feb 17, 2015.

¹⁹ See note 11 above.

As to school bullying in particular (including cyberbullying), the Education Bureau has adopted a “zero tolerance policy”, issued a circular to schools in Hong Kong urging them to implement “positive measures”, given guidelines and advice for schools as well as organised seminars and workshops for the purpose of training teachers.²⁰ With all due respect, this appears to be an euphemistic way of saying that the Education Bureau has effectively done nothing.

On its web page, the SAR Government has given us two pieces of advice (last updated in February 2015).²¹ First, avoid being identified; second, avoid performing distinctive behaviour whenever in open social environment, like being rude in a discussion forum.

In addition, the Privacy Office has published two leaflets in an attempt to educate Internet users: “Cyberbullying – What you need to know”²² (first published in Oct 2014) and “Protecting Online Privacy – Be Smart on Social Networks”.²³ There is no need to discuss them in any detail; suffice to say that they likewise preach self-help.

2.5 Other Jurisdictions: what have they done?

2.5.1 The United Kingdom

According to the Kent Police, there is no law in the UK which specifically deals with cyberbullying.²⁴ Depending on the facts of a given case, various enactments may apply, such as the Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

In October last year, Justice Secretary Chris Grayling put forward a bill which would make “Internet trolls” liable to imprisonment for two years.²⁵ Grayling called the bill “a law to combat cruelty”. “Crude and degrading” and “cyber-mob” are among the phrases that Grayling had chosen – the rhetoric is definitely there. Despite the introduction of this

²⁰ See note 11 above.

²¹ http://www.infosec.gov.hk/english/youngsters/cyberbullying_3.html Retrieved Feb 18, 2015.

²² http://www.pcpd.org.hk/english/publications/files/cyberbullying_e.pdf Retrieved Feb 18, 2015.

²³ http://www.pcpd.org.hk/english/publications/files/SN_e.pdf Retrieved Feb 21, 2015.

²⁴ <http://www.kent.police.uk/advice/personal/internet/cyberbullying.html> Retrieved Feb 16, 2015.

²⁵ <http://www.bbc.com/news/uk-29678989> Retrieved Feb 16, 2015.

bill, it seems that there has been no fundamental change in approach. In other words, UK cyberbullying law remains a “hotchpotch”.

It is truly remarkable that in October 2013, the Welsh government expressed the view that it was better to develop respectful relationships than to criminalise bullying. It had also published “anti-bullying guidance”.²⁶ The overall situation is indeed similar to Hong Kong’s status quo.

2.5.2 Canada

It appears that Canada has no federal law which specifically deals with cyberbullying. Depending on the facts of the case, the federal civil law on defamation and unsafe environment may be applicable. The same is true with respect to the federal criminal law on harassment and “defamatory libel”. Harassment carries a maximum sentence of imprisonment for 10 years, whereas the maximum sentence for “defamatory libel” is five years.²⁷

The Provinces and Territories have different laws on the subject of bullying.²⁸

2.5.3 Australia

According to the Australian Human Rights Commission, each state and territory in Australia has different laws governing the issue of bullying.²⁹ In New South Wales, it is “illegal to use mobiles or the internet in a way that is menacing, harassing or offensive.”³⁰ Offenders are liable to imprisonment for three years. Students who cyberbully their peers could be suspended or even expelled.

²⁶ <http://www.bbc.com/news/uk-wales-24525491> Retrieved Feb 16, 2015.

²⁷ <http://www.prevnet.ca/bullying/cyber-bullying/legal-consequences> Retrieved Feb 16, 2015.

²⁸ See note 27 above.

²⁹ <https://www.humanrights.gov.au/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying-fact-sheet> Retrieved Feb 17, 2015.

³⁰ <http://www.legalaid.nsw.gov.au/publications/factsheets-and-resources/online-social-networking-cyber-bullying> Retrieved Feb 17, 2015.

2.5.4 New Zealand

New Zealand is the most relevant jurisdiction for our present purposes. The Harmful Digital Communications Bill was introduced in 2013,³¹ which squarely confronts the social ill of cyberbullying. It is submitted that Hong Kong has a lot to learn from this model.

The first remarkable feature of the Bill is the preference for informal resolution mechanisms. Under the proposed regime, persons who consider themselves to be victims of cyberbullying must first lodge a complaint with the “Approved Agency”, which will then seek to settle the case through negotiation, mediation and persuasion. Failing that, court proceedings may be initiated.

The second remarkable feature is the Bill’s treatment of online content hosts’ liability. The touchstone is reasonableness.³² Moreover, although non-compliance with a Court order (such as an order to take down materials) is a strict liability offence, the defence of reasonable excuse is still open.³³

Section 19 of the Bill creates the offence of “causing harm by posting digital communication”. Essentially, there are three elements:

- (1) Intention to cause harm;
- (2) Harm has in fact been caused;
- (3) Harm would have been caused “to an ordinary reasonable person in the position of the victim”.

The Bill contains very detailed definitions. At this stage, it is sufficient to note that “harm” is defined as “serious emotional distress” in section 4 of the Bill, while “digital communication” is defined very broadly.

On the whole, this Bill deserves admiration. That said, it is susceptible to two lines of attack. The first attack concerns the definition of “harm”. It is submitted that the Bill’s definition is unduly narrow, and will lead to

³¹ <http://www.parliament.nz/en-nz/pb/legislation/bills/digests/50PLLaw21041/harmful-digital-communications-bill-2013-bills-digest> Retrieved Feb 18, 2015.

<http://www.legislation.govt.nz/bill/government/2013/0168/6.0/096be8ed80c76cca.pdf> Retrieved Feb 23, 2015.

³² See section 20 of the revised Bill.

<http://www.legislation.govt.nz/bill/government/2013/0168/latest/096be8ed80e2ec61.pdf> Retrieved Feb 23, 2015.

³³ See section 18 of the revised Bill.

the absurd situation where a victim of exceptional mental fortitude will not be able to rely on this proposed law for the simple reason that such a victim feels no “serious emotional distress”.

The second attack is that under this Bill, even saying what is true could possibly amount to an offence. This represents an encroachment on the freedom of speech, and defies the rationale of the defence of truth in the law of defamation. This is no doubt a valid concern, and will be addressed in the next section.

3 Arguments Against Legislation – and why we should still legislate

James To Kun-sun and Charles Peter Mok have both raised certain arguments against legislating on cyberbullying, which have been reproduced in the report of the 2010 study cited above.³⁴ It seems convenient to address some of their arguments at this point. Indeed, construing their comments has not been an easy task, and I hope I have done them justice.

First, it has been argued that enforcement of any such laws will be so difficult as to deprive that law of any practical significance. With all due respect, this is not a sound argument. It must not be forgotten that many laws are difficult to enforce – copyright infringement is always rampant, and smuggling is obviously here to stay. It is submitted that the proper approach is to make the law, and then look for effective ways to enforce it.

Second, it has been argued that we should not legislate against cyberbullying because it is too difficult to define “cyberbullying”, and precise definitions are indispensable in the context of creating a criminal offence.

There is some truth in this objection. As noted at the beginning, different people may have different definition of the term “cyberbullying”, and it is unlikely that a consensus will be reached in the foreseeable future. Nevertheless, that does not mean that we cannot devise an acceptable definition. It is submitted that there is no need for the law to look for a perfect definition of “cyberbullying” which will include every single aspect

³⁴ See note 9 above, p 85.

of the behaviour; instead, the law should seek to arrive at an approximation which will be sufficient for achieving the aims of the legislation. Take the New Zealand Bill as an example. It chooses to criminalise “causing harm by posting digital communication” rather than “cyberbullying” as such. In my opinion, Hong Kong can adopt the same solution.

Third, it has been said that proving the necessary intention will be so difficult that the law, even if made, will be meaningless. The short answer to this objection is that it is not an argument at all. Just because it is difficult to invoke a law does not mean that we should not have that law in the first place. This objection is similar to the point about enforcement difficulties. Another solution (which will be further discussed below) is to lower the requirement of mens rea.

In the light of the serious harm that cyberbullying can cause, the above considerations, either taken individually or cumulatively, are not sufficient reason for refusing to legislate.

However, James To raised this further argument: legislating on cyberbullying will jeopardise the freedom of expression.³⁵

Despite the validity of this concern, we must bear in mind the peculiar nature of the Internet as well as the problems which flow from it. In pre-Internet days, even where a person behaves in a public place in a morally objectionable manner, probably only a few people would have seen it. They might mention it to their friends and relatives, but on the whole the number of people who would ever hear about it would still be rather limited. Very often, after a short while, nobody would ever talk about it. Even if the incident had appeared in the newspapers, any news coverage would likely cease in a matter of days. After some time, the information would not be very accessible, unless someone has retained the clippings, or one goes to the library to look at the microfilms. Potential employers would probably not know about it.

Nowadays, such incidents, however trivial, is likely to attract widespread attention in the Internet forums; search engines have also made it very easy to dig up “ancient” information. Moreover, once available on the Internet, the information will be accessible to a large part of the globe. The

³⁵ See note 34 above.

“wrongdoing” may be the same, but the severity of the “punishment” has increased exponentially.

I do not seek to dispute that as a general rule, people are entitled to say what is true. However, freedom of expression is not absolute – it must be balanced against competing interests. It is submitted that in appropriate cases, even so-called “legitimate universal condemnation” ought to be curtailed. After all, any punishment must fit the crime, but in the context of online lynching, it is all too easy to lose sight of the need for proportionality.

It is further submitted that the public interest in the free flow of information can be taken care of by introducing a “public interest defence” in the cyberbullying law. For example, online news media should be allowed to report corruption cases and disclose the names of the officials involved. “Public interest” for the purposes of this defence should not be freedom of expression or similar concepts. Apart from assisting in the proper balancing of competing interests, this proposal has this further benefit: it should be very easy to implement, since pleading “public interest” as a defence is not a concept hitherto unknown to the law – it has long been recognised as a defence to a claim of defamation.

4 What to cover?

Legislation on cyberbullying must achieve three things: first, it must clearly spell out its aims; second, it must offer precise definitions; and third, it must contain specific measures against cyberbullying.

4.1 Aims

The importance of clearly spelling out the aims of the statute must not be underestimated. It assists in interpretation as well as offers a standard against which the effectiveness of the law can be measured.

It is submitted that the legislation should have the following three aims:

1. To deter cyberbullying
2. To provide for the effective and speedy resolution of cases of cyberbullying

3. To mitigate the harm caused to victims of cyberbullying,³⁶ which is arguably the most important aim from the point of view of victims.³⁷

4.2 Definitions

It is submitted that Hong Kong should follow the suggestion made in the New Zealand Bill, and criminalise “causing harm by posting digital communication” rather than “cyberbullying” as such. However, for the sake of convenience, “cyberbullying” can be adopted as a short-hand term and defined as “causing harm by posting digital communication”.

It is further submitted that the three elements of the offence given in section 19 of the New Zealand Bill should be adopted in Hong Kong, subject to the modification that recklessness shall be sufficient mens rea. This recklessness limb is truly important – very often in modern cases, what can be observed is a callous disregard for the feelings of others rather than an intention to do harm. This is especially true in the context of the practice of “sharing”, such as retweeting. Without this limb, victims may not in fact receive much protection. However, it is submitted that in accordance with the general principles of the criminal law, mere negligence should not be sufficient mens rea; in other words, no person shall be exposed to criminal liability merely because he ought to have known that what he did would cause harm.

I further propose that the same definition of “cyberbullying” should apply for the purposes of the civil law, except that in a civil action it shall be sufficient for the plaintiff to prove negligence (as the term is used in the preceding paragraph).

In cyberbullying cases, what aggravates the damage is the further dissemination of the materials in question, and the law must offer a sufficient response to this phenomenon.³⁸ One benefit of the proposed definition is that it can easily cover acts of dissemination, including forwarding and posting second-hand materials.

³⁶ See section 3 of the NZ Bill.

³⁷ See also 2014 article “Does Australia need tougher cyberbullying legislation?” <http://rightnow.org.au/topics/children-and-youth/does-australia-need-tougher-cyberbullying-legislation/> Retrieved Feb 17, 2015.

³⁸ See <http://www.theage.com.au/news/national/law-lags-behind-cyber-bullying/2007/05/16/1178995236283.html> Retrieved Feb 19, 2015.

In addition, I propose that the cyberbullying law should draw no distinction between minors and adults.

As to the definition of “harm”, it is submitted that it should include fear, distress, physical, psychological, social and academic harm, harm to reputation and harm to property.³⁹

“Digital communication” should be defined as “any form of electronic communication, and includes any text message, writing, photograph, picture, recording or other matter that is communicated electronically.”⁴⁰

“Internet service provider” (“ISP”) should include any person who has control over the part of the electronic retrieval system (such as a website or an online application) on which the communication is posted and accessible by the user.⁴¹

“Posting” should include transferring, sending, publishing, disseminating, and otherwise communicating by means of a digital communication.⁴²

4.3 Specific Measures

4.3.1 Broad Principles

Three broad principles should be mentioned before we go into the specific proposals.

First, it must be remembered that legislating on cyberbullying involves a fine balancing exercise between the freedom of expression on the one hand and the protection of individuals on the other. We must also bear in mind the exceptional power of the Internet to do harm to individuals.

Second, abuse of the proposed law (especially for political purposes) must be guarded against.

Third, the emphasis of the cyberbullying law should be on criminal rather than civil liability. The reason is that civil claims are not always feasible due to the nature of cyberbullying. Consider bullying in online forums.

³⁹ Based on the Ontario Education Act, as cited in <http://www.prevnet.ca/bullying/cyber-bullying/legal-consequences> Retrieved Feb 16, 2015.

⁴⁰ See section 4 of the NZ Bill.

⁴¹ See note 40 above.

⁴² See note 40 above.

Often many people are involved, with differing degree of participation. In the end, harm results. Difficult questions then arise: should liability be joint and several? Given the sheer number of defendants, how is the Court going to assess their respective culpability? If liability is joint but not several, then the administrative difficulties will be even more formidable. How many contribution notices will need to be served? How many third-party proceedings will need to be issued? Can the case even proceed to trial? Contrast all these with criminal proceedings, where even if the government cannot prosecute all the wrongdoers involved, that offers no defence.

4.3.2 What ought to be done?

It is submitted that Hong Kong should follow New Zealand's example and establish a special body (an "Approved Agency") tasked with the informal resolution of cyberbullying cases. The legislation should also stipulate that a court may refuse to exercise its jurisdiction in a cyberbullying case where the plaintiff has not previously filed a complaint with the Approved Agency.

4.3.2.1 *Against ISPs*

To begin with, courts should be given the power to order Internet service providers to take down offending materials. However, enforcement issues may arise as the ISPs in question may be operating in a foreign jurisdiction. It is submitted that the law should *not* resort to shutting down the whole website in an attempt to compel compliance, even where the foreign ISP has been recalcitrant. Such a measure would seriously affect legitimate users; moreover, it would unduly restrict the free flow of information. The effectiveness of such a measure is also highly doubtful, since the tech-savvy can easily bypass government firewalls (as China's experience can confirm). What is worse is that going too far will jeopardise Hong Kong's international reputation as a free and liberal city. Perhaps the best solution is to seek help from those foreign jurisdictions. Global awareness of cyberbullying is on the rise; if they refuse to assist, that will reflect badly on them.

The legislation may also impose an obligation on ISPs (especially online forums) to monitor the materials that they host, but the feasibility of

such a law will be rather uncertain. If liability is strict, then it may not be possible for ISPs to comply with the law without incurring unsustainable costs of operation. Websites may need to be shut down as a result. On the other hand, if the law only requires that reasonable steps be taken by ISPs, then the law might be practically useless where cyberbullying is truly rampant. That said, it is submitted that this measure is worth a try, even though its utility may be rather limited.

4.3.2.2 Against Cyberbullies

As discussed above, cyberbullying should be made a criminal offence. Apart from that, it is submitted that the legislation should offer clear sentencing guidelines without limiting judges' discretion to depart from such guidelines where appropriate. I propose that probation and bind-over should be open to the judge. Imprisonment should also be available, but should not be lightly resorted to; after all, it is mutual respect rather than deterrence which goes to the root of the problem of cyberbullying, and imprisonment is likely to cause even more hatred and bitterness.

As to the most proper maximum sentence, it is submitted that Hong Kong should follow the English approach and set the maximum at two years. This will allow sufficient flexibility to deal with the more serious cases, and will hopefully send a clear message to Hong Kong's "netizens". Such a message would seem particularly apt in view of the worsening trend of cyberbullying in this city.

In respect of civil liability, the legislation should specifically create a new cause of action known as "cyberbullying", and provide clear rules on the assessment of damages. While cyberbullying is an intentional wrongdoing, victims should also be expected to show reasonable mental fortitude. It is submitted that the rules on remoteness of damage should apply to an action for cyberbullying. This will sit comfortably with the rules governing the award of damages for assault and battery, which also take into account remoteness.⁴³ For the avoidance of doubt, the legislation should clearly state that the suicide of a victim shall be

⁴³ Halsbury's Laws of Hong Kong, para 380.317.

regarded as a distinct type of damage, which will not be recoverable unless it was reasonably foreseeable when the bullying took place.

Injunctions should also be available; for example, the Court may make an order to the effect that the defendant must not contact the victim for a number of years or that the defendant must destroy all offending materials in his possession.

However, it is submitted that no punitive damages should ever be granted, since punishment should remain the province of the criminal provisions of the cyberbullying law.

5 Conclusion

Legislation on cyberbullying is long overdue. It is hoped that change will come soon.