Why Hong Kong Should Legislate on Cyberbullying

Introduction

Although there may be many different definitions, cyberbullying is defined by Merriam Webster as “the electronic posting of mean-spirited messages about a person… often done anonymously.” Cyberbullying has become an increasingly serious problem worldwide, including in Hong Kong. A survey conducted by the Hong Kong Federation of Youth Groups in 2010 among Hong Kong secondary students showed that around 30% of the 2981 respondents had been cyberbullied while 57% of the respondents had witnessed cyberbullying. The number has only increased in the past five years as the Office of the Privacy Commissioner recently announced that the number of reported cyberbullying cases had drastically increased, from six in 2013 to thirty four in 2014. However, most of these cases had been dropped due to problems faced by officials.

In many ways, cyberbullying is a more serious problem than traditional bullying, with studies showing that victims of cyberbullying suffer greater harm than traditional victims. Research shows that teens who have been cyberbullied are more depressed, have greater social anxiety, decreased self-esteem, and are two times more likely to attempt suicide than their non-bullied peers. There are various reasons as to why cyberbullying is more harmful than traditional bullying. First, the Internet allows people to act anonymously, giving them freedom to say anything they want without fear of retribution. Moreover, cyberbullying can be spread widely instantly and removal is almost impossible. While it may be possible to request the service provider to take down the material, it would most likely have already been seen and shared by many. Often, the platforms on which cyberbullying is committed is beyond the reach of adults, as adults may not have access to these platforms. Finally, the most significant aspect of cyberbullying is that it is not limited to school but is “never-ending.” Unlike traditional bullying, victims cannot escape cyberbullying and home is no longer a refuge. Many adults believe that

1 “Hong Kong seeks a spike in cyberbullying cases”, RTHK, 27 January 2015.
2 Marilyn A. Campbell, Barbara Spears, Phillip Slee, Desmond A. Butler, and Sally M. Kift, “Victims’ Perceptions of Traditional and Cyberbullying, and the Psychosocial Correlates of Their Victimization” (2012) 17 Emotional and Behavioural Difficulties
3 Sameer Hinduja and Justin W. Patchin, Bullying beyond the schoolyard: Preventing and responding to cyberbullying (Corwin Press, 2009).
victims can escape such bullying by staying off the Internet. However, such a “solution” is impracticable, given the fact that the Internet has become an indispensable part of life. Moreover, even if the victim avoids the materials online, these materials may be viewed by the victim’s classmates, who will only continue the bullying physically.

This paper seeks to argue the pressing need for Hong Kong to legislate on cyberbullying. First, the paper will go through the current status of the law on cyberbullying in Hong Kong and the unsatisfying use of tort law as an alternative mechanism for remedy. Then the paper will go through some arguments made against such legislation and why, despite such opposition, Hong Kong should nevertheless legislate and in what manner, drawing examples from other jurisdictions that have already enacted such legislation.

**Current Status of Hong Kong**

In Hong Kong, there is currently no statute on cyberbullying. If such actions involve criminal offences, such as blackmail, then these conduct will be governed by the relevant legislation. Victims can also pursue civil remedies, such as through tort law. Victims may also have recourse if cyberbullying activities breach any provisions of the Personal Data (Privacy) Ordinance or the Data Protection Principles (DPPs). For example, DPP1 states that personal data can only be used for lawful purposes whereas DPP3 states that personal data should only be used for the original purpose it was collected for and that use of data for new purposes requires consent. Although violating the DPPs is not an offence, the Privacy Commissioner can serve an enforcement notice on the contravener and failure to comply with such notice will constitute an offence. Violators may be liable to a fine of $50,000, and a daily fine of $1000 in a continuing offence, and imprisonment for two years.

In light of the increasing number of cyberbullying cases, the Office of Privacy Commissioner for Personal Data also issued two leaflets regarding cyber-activities in 2014.

**The Use of Tort Law**

Victims of cyberbullying can seek remedies by commencing actions in tort law, such as defamation. However, this is not a very efficient mechanism for victims of cyberbullying. The most basic objections are that such proceedings are time consuming, costly and very emotionally draining, with only few cases of success. Given that most victims of cyberbullying are young children and their vulnerability, proceedings through tort law is unlikely to be very appropriate. Instead, issues of
cyberbullying should be dealt with at school or at home as much as possible, with courts being used as a measure of last resort.

In addition, victims may face many problems when commencing actions in tort. First of all, many perpetrators of cyberbullying act anonymously and are, therefore, very difficult to identify without obtaining such information from service providers, which in itself is a difficult task. Moreover, cyberbullying often occurs at the hands of a group of people. Therefore, if the victim can identify these people, he must decide whom to sue or if possible, sue the whole group. However, problems are exacerbated when these people are spread out all over the world. Furthermore, many judges tend to not view a victim’s injury as amounting to tort or may be unwilling to impose liability on bullies who are young.

Lastly, even if proceedings were successful, bullies may not even have adequate resources to properly compensate the victim.

**Should Hong Kong Legislate on Cyberbullying?**

**Arguments Against Legislation**

Legislating on cyberbullying is a very controversial subject and has faced criticism and opposition from many.

One of the largest fears is that such legislation would potential infringe upon the fundamental right of freedom of speech. Certain courts have also echoed this concern. For example, the New York Court of Appeal held, by majority, that the New York cyberbullying statute was unconstitutional as it violated the right to free speech⁴.

The right to free speech is also constitutionally guarded in Hong Kong under Article 27 of the Basic Law and has been guarded zealously. Such concerns usually stem from the fact that cyberbullying legislation are generally framed in broad terms. For example, the US state of Louisiana defines cyberbullying as

“the transmission of any electronic textual, visual, written, or oral communication with the malicious and willful intent to coerce, abuse, torment, or intimidate a person under the age of eighteen⁵.”

The US state of Oregon defines cyberbullying as

“the use of any electronic communication device to harass, intimidate or bully⁶.”

---

As shown, although different jurisdictions define cyberbullying differently, the common theme is that most provisions use very general terms. The use of such vague terms causes confusion to enforcement officials, usually teachers and schools, as to the exact scope of their powers to restrict speech in cyberbullying cases. Many often have a difficult time distinguishing between permissible and impermissible speech. Moreover, it is often uncertain as to how much a school can regulate off-campus speech, which constitutes the majority of cyberbullying.

Another source of concern is the risk of over-criminalising and imposing punishment disproportionate to the offence. Some argue that existing legislation can sufficiently deal with cyberbullying, such as pursuing an action in tort law, as mentioned above, and under the Personal Data (Privacy) Ordinance. Without sufficiently certain drafting, many are worried that the criminal sanctions would be disproportionate to perpetrators of cyberbullying, which are generally students. Many bullies, feeling emboldened by the anonymity provided by the Internet, frequently write hateful comments without thoughts as to the law. The introduction of cyberbullying legislation would only result in many students finding themselves with a record for doing something thoughtlessly and that most of their peers do as well.

Legislating on cyberbullying may also increase the burden on the police, as people would call on the police to deal with all sorts of cyberbullying cases, both minor and serious. If forced to investigate minor cases, this may shift efforts and resources away from more serious cases, including more serious cyberbullying cases.

Some may suggest that Hong Kong should adopt a real-name system, such as those used in South Korea (“Korea”) and, more recently, the People’s Republic of China (“China”). Korea first introduced the Real Name Registration System in 2008 in an attempt to curb cyberbullying. Under the system, users, who wanted to comment on news media sites with more than 100,000 visitors per day, had to register with their real names. After registration, users could operate under a pseudonym but their real identity could be disclosed if law enforcement officials required them. Moreover, if victims of cyberbullying wanted to sue their bullies,

---

8 Lyrissa Lidsky and Andrew Pinzon Garcia, “How Not to Criminalize Cyberbullying” (2012) 77 Mo. L. Rev. 693
9 Ryan Broll and Laura Huey, “‘Just Being Mean to Somebody Isn’t a Police Matter’: Police Perspectives on Policing Cyberbullying” (2014) Journal of School Violence
portal sites would be required to disclose the bullies’ personal information, such as their names and addresses. Recently, China has also introduced a similar registration system among microblogging sites.

**Examples of legislation abroad**

With the increasing number of cyberbullying cases, various jurisdictions have either taken steps to deal with the problem by issuing specific legislation or are seeking to introduce such legislation.

**Canada**

Many provinces in Canada have already put in place legislation to deal with cyberbullying. After a tragic cyberbullying incident, which resulted in a teen’s death, the province of Nova Scotia enacted the Cyber-Safety Act in 2013. The act allows victims to obtain “protection orders” against their bullies and may require their perpetrators to identify themselves.\(^\text{10}\) Victims can also bring actions against the parents of perpetrators if they are under 18.\(^\text{11}\) Additionally, a specialised police unit was established to deal specifically with cyberbullying cases.

Ontario also amended its Education Act to require schools to provide instructions to its students on bullying, remedial programs for victims, and programs to teach teachers on dealing with bullying. In addition to these two provinces, many other provinces have enacted local legislation to deal with cyberbullying.

Moreover, a federal cyberbullying bill (Bill C-13, Protecting Canadians from Online Crime Act) was introduced to Parliament in November 2013. The act provides police with more extensive powers to investigate cyberbullying cases, such as the right to seize electronics used. The Act also allows the police to track cyberbullying perpetrators. Although the bill has been quite controversial\(^\text{12}\) and raised concerns about giving police too much power to police to conduct surveillance and access private information, the Bill received Royal Assent in early December 2014.\(^\text{13}\)

**United States**

Although there is no federal anti-cyberbullying legislation, most US states deal with cyberbullying through their state legislation. California was the first state to enact legislation regarding cyberbullying in 2008. Currently,
all states, except Montana, have enacted some type of anti-bullying legislation. 47 states have laws, which include terms such as electronic harassment or bullying electronically. 21 states have specifically included cyberbullying and ten of those 21 states impose criminal sanctions for cyberbullying.\textsuperscript{14}

In 2009, a federal cyberbullying bill (Megan Meier Cyberbullying Prevention Act) was proposed but failed to pass due to strong objections. The Act proposed to make cyberbullying a federal offense, whereby anyone who used electronic means to harass, intimidate, or cause substantial emotional distress to a person would have been liable to a fine or two years imprisonment.

**South Africa**

In 2013, South Africa became the first country in Southern African to enact cyberbullying legislation. The Protection from Harassment Act\textsuperscript{15} allows victims of cyberbullying to apply for a protection order against their bullies\textsuperscript{16} and perpetrators can be liable to a fine or an imprisonment term of up to five years.\textsuperscript{17} Moreover, the Act also requires service providers to hand over information regarding the perpetrator, including his name and address, if law enforcement officials require them.\textsuperscript{18} Failure to do so may result in the service provider being liable for a fine not exceeding R 10,000 or its staff being liable to six months imprisonment.

**New Zealand**

New Zealand is seeking to pass the Harmful Digital Communications Bill\textsuperscript{19} in order to protect victims of “harmful digital communications,” including text messages, pictures, and other electronic communications.\textsuperscript{20} Perpetrators may be prosecuted if they cause serious emotional distress to the victims and may be liable for a fine of $2000 or imprisonment of three months. The Bill would also create a specialised enforcement agency to deal specifically cyberbullying cases.

Under the bill, a double-tiered enforcement regime is proposed. The first tier will involve the appointment of an approved agency to deal with the

---


\textsuperscript{15} Act 17 of 2011.

\textsuperscript{16} Ibid, s. 2.

\textsuperscript{17} Ibid, s. 18.

\textsuperscript{18} Ibid, s. 4.

\textsuperscript{19} 2013 (168 – 2).

\textsuperscript{20} Ibid, cl 3.

\textsuperscript{21} Ibid, cl 4.
cyberbullying case and attempt to remedy the problem without involving the courts. More serious cases or cases that cannot be resolved amicably will be moved to the courts, the second tier.

The United Kingdom

The UK does not have any specific legislation regarding cyberbullying. However, UK legislation requires schools to have in place anti-bullying policies, including cyber-bullying, as will be explained further below. Perpetrators can only be prosecuted under the Malicious Communications Act for sending sexually offensive, verbally abusive, or threatening material on the Internet, for which the maximum sentence is six months imprisonment. Moreover, similar to the situation in Hong Kong, cyberbullying may be dealt with under existing UK criminal laws if it involves the relevant activity, such as threats and harassment.

However, there have been calls upon the government to legislate specifically on cyberbullying. Currently, the Criminal Justice and Courts Bill is before Parliament. Under this Bill, magistrate courts will have the power to transfer more serious cases to higher courts and the maximum sentence under the Malicious Communications Act may be increased from six months to two years. Police will also be given more time to obtain evidence in building cyberbullying cases. This will be a welcome development as the Malicious Communications Act was enacted more than ten years ago, before the explosive popularity of social networking sites such as Facebook and Twitter.

In addition, in November 2014, the Irish Law Reform Commission called for public opinion on whether Irish criminal law should be amended to address the problem of cyberbullying through their Issue Paper on “Cyber-Crime Affecting Personal Safety, Privacy, and Reputation, including Cyber-bullying.”

Arguments for legislation

Despite certain valid arguments against legislation, it is argued that Hong Kong should, nevertheless, legislate on cyberbullying. The advantages of and the pressing need for such legislation outweighs any possible disadvantages. With the ever-increasing development of technology and the pervasive use of such technology in everyday life, governments can no longer avoid the problems that come with the use of such technology. Without intervention through legislation, the problems surrounding cyberbullying will only increase. Instead, it is argued that any

22 “Crackdown on the Cyber-Mobs Poisoning Britain: Sentence for Web Trolls to be Quadrupled to Two Years After Shocking High-Profile Online Abuse Cases”, *The Daily Mail*, 18 October 2014.
cyberbullying legislation should be supplemented with governmental support in establishing education programmes in all schools. The combination of legislation as a deterrent and educational and preventive programmes will be able to combat cyberbullying to a better extent rather than the independent use of each method.

Although the exact wording of such legislation can only be completed after careful and extensive consultation with the public and relevant experts, this paper will suggest a few points that drafters should take into account when drafting such legislation.

Much of the objection stems from the fear that it would infringe upon the fundamental right to free speech. While the paramount importance of free speech is acknowledged, the government’s duty to protect children is also a very compelling point. All jurisdictions demonstrate the government’s interest in protecting the young and vulnerable by implementing legislation and criminalising activities that harm children, such as physical abuse or sexual exploitation. While cyberbullying may not generally cause physical harm, it is still very mentally harmful to children, even resulting in teen suicides. The fundamental right to free speech is not absolute and is already subject to certain exceptions, such as libel, public order, and discrimination. It is doubtful why a child’s right to be protected from cyberbullying is not sufficient a justification to infringe upon, to a slight extent, a child’s speech.

Certainly, clear boundaries will have to be set within the legislation to ensure that the legislation does not overstep onto the constitutional right. For example, the law should only interfere when cyberbullying is done repeatedly, consistently, and to an excessive point where it warrants such intervention. It is understandable that cyberbullying committed on a daily basis over a long period of time warrants such legal intervention, as opposed to a single instance of name-calling. Drafters will have to carefully balance between protection of victims of cyberbullying and the right to free speech. Therefore, it seems that the argument of infringement of free speech is not an adequate reason in itself to completely oppose the enactment of such legislation.

Examples of attempts to balance the two rights can be seen abroad. For example, Louisiana’s statute attempts to prevent too much infringement by expressly stating that its cyberbullying provisions cannot be used “to prohibit or restrict religious free speech.” While this may not be a perfect example, it shows that the two rights can coexist, if done correctly.

Drafters may also have to overcome the difficulty of defining “cyberbullying.” It is argued that the definition should not be too narrow, as it would very likely cause the legislation to be rendered useless. Given the rapidly developing nature of technology, any narrow definition, although it may give certainty at the time, will soon become out-dated. It would be more useful for a broad definition of “cyberbullying” to be adopted. Although such a definition may cause ambiguity and confusion at first, it is predicted that subsequent judiciary decisions will help narrow down and clearly delineate the boundaries and the scope of the legislation. Some may, then, bring up the valid point of whether there is a need for legislation at all, given that it may be sufficient to leave the issue of cyberbullying in the hands of the capable Hong Kong judiciary. However, it is a fundamental principle that the role of the judiciary is to interpret the law, rather than make new law. Therefore, the first step should be taken by the legislature by enacting a new legislation. Afterwards, the judiciary would play a paramount role in clarifying and interpreting the legislation. Given the competence of and the amount of public confidence the judiciary receives, the public can expect to receive more clarity from the subsequent development of case law.

Some jurisdictions abroad, in addition to having legislation to deal specifically with cyberbullying, also criminalises cyberbullying. For example, the US states of Arkansas\textsuperscript{24}, Idaho\textsuperscript{25}, and Louisiana\textsuperscript{26} criminalise cyberbullying. The province of British Columbia, Canada, also imposes fines and imprisonment in its cyberbullying legislation and provisions.

Whether Hong Kong, if it chooses to enact such legislation, would follow the footsteps of these states is unclear. However, if drafters choose to impose criminal sanctions on cyberbullying, such punishment should only be used as a measure of last resort and very rarely.

If cyberbullying is criminalised, a distinction should be made between adult and child perpetrators. In most cases of cyberbullying among students, the child perpetrators, generally, are unaware of the consequences of their words and actions online. Feeling emboldened by the lack of face-to-face interaction and the anonymity that the Internet provides, children often write and say things that they generally would not be able to say offline. Given the mental vulnerability of such children, it is not suggested that fines and especially imprisonment terms be easily imposed on them. For example, Louisiana only imposes liability when cyberbullying is carried out against child victims. Child perpetrators are

\textsuperscript{24} Ark. Code Ann. § 5-41-108(a).
\textsuperscript{25} Idaho Code § 18-7906.
treated more leniently than adults and children under the age of 17 are not dealt with under the regulate statute, but instead under a special “Children’s Code.” Similarly, Hong Kong should make such a clear distinction when drafting such legislation.

Additionally, some jurisdictions, such as Alberta, Canada, imposes a duty on witnesses of cyberbullying to report such incidents, failure of which could lead to suspension or expulsion. However, it is suggested that Hong Kong should not take a similar stance. Given the already controversial nature of cyberbullying laws, the inclusion of such obligations would most likely decrease public support. Moreover, the imposition of liability on mere witnesses will result in a massive surge of cases, which may overburden the police and courts. Enforcement officials will also be overburdened, as their workload in monitoring and identifying these witnesses will significantly increase. The scope of the potential class of offenders would simply be too large. Moreover, it would be unfair to the witnesses. Witnessing students often do not stand up for the victims or report the incident to adults for many reasons. They may not report the incident to teachers or adults because they feel that even if they did, they would not be able to do anything. Students often, also, fail to report such incidents for fear of being labelled as a “snitch” or becoming the new target of such bullying. Therefore, imposing liability on these students would only result in an increase in prosecution and would not act as much as a deterrent as opposed to education and changing the mentality of students. In general, the disadvantages and burdens caused by imposing such liability would greatly outweigh any deterrent effect it may have.

In imposing criminal liability, care should also be taken so as not to overburden the police and law enforcement officials, as mentioned above. The law must clearly set out a distinction between minor cases and more serious cases that actually warrant police intervention. In fact, it is suggested that a specialised enforcement agency be established to deal solely with cyberbullying cases. By having specialised enforcement officials, cases can be dealt with in a more efficient manner.

Lastly, while most cyberbullying cases occur among students, drafters should remember that teachers and school staff could also be targets of

28 Maryland (Md. Code Ann, Educ. § 7-424(b)), Mississippi (Miss. Code Ann. § 37-11- 67(4)), and South Carolina (S.C. Code Ann. § 59-63-130(B)).
29 Education Act, SA 2012, c E.03, s. 31(e).
30 Ibid, s. 36(1)(a).
31 Ibid, s. 37(1)(a).
cyberbullying. Therefore, the legislation should also provide adequate protection for this group of people as well.

Legislation may be able to serve as a deterrent but, by itself, would not be able to address the root cause of the problem. While legislation is important as the first stepping-stone, what is equally important is the combined use of educational and preventive programmes in schools, which the government should supply adequate funds for. The establishment of such programmes can be required by legislation and this has been done in certain jurisdictions, such as the UK. In the UK, there are two sets of relevant laws in the cyberbullying context. The School Standards and Framework Act 1998 requires all schools to have in place anti-bullying policies, including cyberbullying. The Education and Inspections Act 2006 also gives teachers and schools more power to enforce such policies and regulate students’ conduct outside school. Many US states also require the establishment of such policies within schools.33

Such programmes would be necessary to not only educate children on the safe usage of the Internet but also prevent cyberbullying from occurring. These programmes should also educate parents on cyberbullying, such as monitoring their children’s online activities and picking up on clues that may indicate that their children may be victims of cyberbullying. However, the sole responsibility should not lie with parents. Nowadays, there are many single-parent families and, especially in Hong Kong, families where both parents work. In such families, it may be difficult for parents to constantly monitor what their children have been doing online. Moreover, many parents may find difficulties in accessing and understanding the platforms and sites used by their children.

Schools should have in place appropriate bullying policies and provide adequate training to its teachers and staff. If this is to be mandated by legislation, the powers and responsibilities of schools and teachers must be clearly delineated so as not to cause further confusion. If the powers and duties are not clearly set out, schools may be confused as to whether a certain actions and cases of cyberbullying are within the scope of their power and will significantly decrease the effectiveness of such legislation. Moreover, schools should also be expressly given the authority to deal with off-campus speech and cyberbullying, as cyberbullying generally takes place outside the school.34

33 Montana, New York, Alabama, Alaska.
In addition, schools must also have in place appropriate remedial mechanisms, such as appropriately trained counsellors, whereby victims of cyberbullying can receive help and support.

The government must also work together with schools and relevant organisations to raise awareness of the issue of cyberbullying among the Hong Kong public. For example, Canada annually hosts an Anti-Bullying Day, whereby supporters wear pink, blue or purple to demonstrate their support against bullying. In 2007, the US Advertising Council, along with various other governmental departments, launched a new public service advertising campaign so as to educate teens on preventing and standing up against cyberbullying.

Lastly, a real name registration system, as mentioned previously, is unlikely to be of any use and is most likely to be held as being unconstitutional by infringing the right to freedom of speech. In fact, Korea has abolished this system after a unanimous decision by the Korean Constitutional Court in 2012. The court was of the opinion that the benefits to the public were not sufficient enough to justify the restrictions imposed on the right to free speech. Such a restriction discouraged people from criticising the government or other influential groups because of their fear over punishment. The court acknowledged the harms that could arise from online anonymity, but priority should be accorded to safeguarding the constitutional right to free speech. The recent introduction of such a system in China has also been subject to much criticism, as it is seen as a precursor to even more stringent censorship and monitoring of speech, especially those that are harmful to the country’s authorities.

Given the lack of national and political boundaries within the Internet, it is important that Hong Kong deals with cyberbullying with other jurisdictions. The European Union is a good example of such regional effort. The Council of Europe has acknowledged the growing problem of cyberbullying and has issued several documents on it. Moreover, in 2009, the EU has also worked with SNS providers and NGOs to publish the “Safer Social Networking Principles for the EU.” These principles provide SNS providers and other similar sites with practice guidelines so as to provide a safer environment for children.

---

35 2010 Heon Ma 47, 252
36 The Recommendation on empowering children in the new information and communications environment (Council of Europe, 2006); The Declaration on protecting the dignity, security and privacy of children on the Internet (Council of Europe, 2008); The Recommendation on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Council of Europe, 2009); The Recommendation on the protection of human rights in social networks (Council of Europe, 2012)
Another initiative was launched in January 2012 whereby the Information and Communication Technologies (ICT) coalition worked with 25 companies, including Facebook and Google, to issue “Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU.”

Similarly, Hong Kong should seek to work together with other jurisdictions to come up with initiatives and regimes to combat cyberbullying, which can frequently happen cross-border.

**Conclusion**

Although there may be valid reasons for opposing legislation on cyberbullying, such as privacy issues and rights to free speech, Hong Kong should legislate on cyberbullying as soon as possible. Cyberbullying is a growing and serious problem and must be dealt with before the negative effects grow more severe. The first step in the right direction would be to legislate upon the matter and subsequently, be followed with the combined use of educational and preventive programmes within schools. Together, the two should be able to effectively combat cyberbullying and prevent more harm to and suicides of children and adults alike.