Cybercrime and its Child Victims: Risks and Resolutions

Views from Against Child Abuse

(Sexual exploitation online, cyber sexual grooming, online pornography, and cyber bullying)

Submitted to Law Reform Commission of Hong Kong

22 October 2019

Introduction

1. Against Child Abuse (ACA) was established in 1979 as the only charitable organisation specialized in child protection in Hong Kong. ACA is committed to protecting children and promoting child welfare. We strive to eliminate all forms of child abuse.
2. ACA has been very concerned at developing dangers to children and young people in cyberspace, and which now require solutions. We submit our views herewith.
3. Cybercrime is rampant around the globe and poses real challenges to the rule of law. In the digital age, cybercrime challenges governments, businesses and individuals alike, but it is often the most vulnerable members of society who are at the greatest risk. Although governments and businesses can take measures to safeguard their operations, greater protections are required for those who are least able to defend themselves. All too often, their interests do not receive the prioritization they deserve, and existing laws have not always moved with the times.
4. Human traffickers can use the internet to traffic children, and to ensnare victims. Migrant workers, for example, are sometimes being defrauded by bogus employment agencies, finding themselves ending up as the victims of debt bondage and trafficking. Cybersex, often involving young people, is a huge global industry, with much of it being arranged over the internet by anonymous traffickers who need not fear of being caught in a police raid, as was once the case.
5. Bullying is common in many sectors of the society. Effects on bullied children and the young are ramified many times in the cyberspace. Harm from bullying can result in self-destructive acts by the bullied.
6. The Hong Kong Family Planning Association releases its results on Youth Sexuality Study every 5 years. The 2016 report revealed that 33% female 59% male secondary school students had viewed sexual materials, a 5% increase from 2011 report. And 15% of male students had watched sexual materials over 15 episodes in the previous month. Overall, 15-20% of the respondents had ever received sexual messages in their mobile phone, in word descriptions, pictorial, or videos formats. 34-43% of the females blocked such messages from senders, whereas 24-29% of the males had saved such messages.
7. In Singapore, the DQ Institute, an international think tank created to improve digital education, conducted a survey in 2017 in Singapore among 3,600 children, aged between 8 and 12. The survey discovered that 54% of children in this age category had been exposed to at least one cyber risk, including cyberbullying and online sexual behavior, but

also offline meetings. For those exposed to these risks, 43% had faced cyberbullying in the previous year. Moreover, 16% had been involved in online sexual behavior, such as having searched for and/or visited websites with sexual content, and/or having had sexual conversations online with complete strangers. About 1 in 10 of the respondents said they had chatted with and met online strangers in real life. So how can children be protected, both generally, but also specifically from exploitation? The first area for consideration is child exploitation online.

8. In October 2019, lawmakers in Mainland China are working to revise the Minors Protection Law for citizens under 18, codifying the protection against cyber-based crimes and addictions. Such revision is as a major move in internet governance. The 11-clause new chapter named "Internet Protection", lays out duties for governments, schools, parents and digital service providers as to their responsibilities in navigating youngsters through cyberspace. Such draft revision has put the protection of juveniles against online pornography, violence and bullying in a more prominent spotlight, which could have long-lasting social benefits.
9. Our prime concern is with criminality which involves children, and this is an area where new laws are urgently needed. In this paper, we focus on sexual exploitation online, cyber sexual grooming, online pornography, and cyber bullying.

Child Sexual Exploitation Online

10. In 2003, Hong Kong **enacted** its Child Pornography Ordinance, and this has helped to combat child imagery online. A person who makes, produces, publishes or advertises child pornography faces up to 8 years' imprisonment and a fine of HK$2,000,000. Someone convicted of possessing child pornography is liable to imprisonment for 5 years and a fine of $1,000,000.
11. In applying this law, the judges have emphasized that their sentences must punish the offender and deter others of a like mind, and substantial sentences of imprisonment are regularly imposed upon offenders. Although this law has helped to protect children from sexual abuse, global restrictions designed to protect children are often inadequate, or cannot be enforced.
12. Sexual abuse of children is occurring on online platforms, often involving children from Southeast Asia. It is essential that the social media companies and search engines treat child sexual exploitation as seriously as terrorism, and stop such images ever being uploaded. Although, for example, Microsoft's PhotoDNA technology is now using artificial intelligence to locate and remove child abuse imagery online, the threats are evolving faster than the industry's response. Some companies, moreover, are still not taking the dangers sufficiently seriously, and must do more. Algorithms, for example, must be adjusted to make it harder to find child pornography in search results. It is necessary, therefore, for responsible governments everywhere to ensure that internet companies, whether in Silicon Valley or elsewhere, take all possible measures to eliminate child pornography from their networks.

Cyber Sexual Grooming

13. Sexual grooming online is another concern. The Social Welfare Department has kept a Child Protection Registry on abuse cases including sexual abuse. Sexual Grooming has recently been added in the registry. As more cases come to light when children fall victim in the internet, meaningful official data in Hong Kong might illustrate the scale of the problem.
14. In the United Kingdom, it was reported in February 2019 that the number of cybersex offences against children had trebled over the last three years, increasing from 3,186 to 9,543. The Office for National Statistics found that cyber-related crimes comprised 16 % of child sexual offences recorded by the police in England and Wales in 2017-2018. In the UK, a new offence of sexual communication with a child was introduced in 2015, which is designed to combat the sexual grooming of children by pedophiles online, and there were over 3,000 offences discovered in its first full year of operation. It has, moreover, been discovered that Facebook owned Apps, including Instagram and WhatsApp, accounted for half of the cases of sexual communication with a child. What this means, therefore, is that the social networks have to take more responsibility by stopping their networks being used as gateways for crimes against children. The social networks must create safe accounts for children, and take proactive steps to stop online grooming.
15. In 2016, the Law Reform Commission of Hong Kong recommended the creation of a **new offence** of sexual grooming involving children. This is intended to protect them from pedophiles who might try to groom them by communicating with them on a mobile phone or on the internet to gain their trust and confidence, with the intention of sexually abusing them. This proposal is still being discussed, but once it is enacted it will help Hong Kong to protect its children from a very real danger. However, it will not be easy, as sexual predators make use of social networks to identify victims, and they know how to avoid detection by changing their tactics.
16. However, there are sometimes warning signs, and the technology companies must be required to police their platforms comprehensively. They could, for example, closely monitor a large number of friend requests to a particular child, or intervene when there is no obvious connection between the parties. If anonymization techniques are being used by the person who is contacting the child, this may well be an indication that all is not as it should be. With the right technology, including artificial intelligence, it should be possible for the industry to identify sexual grooming activities and locate those responsible. It is the largest sites which have the biggest problems, and the technology companies must be proactive in addressing them. If, therefore, a statutory duty of care were to be imposed on social media firms, requiring them to do everything possible to protect children online, this could help to reduce the risks they face. The technology companies must protect children from harmful content, such as cyberbullying, sexual content and abuse, and prevent under-age children from joining their sites.

Online Pornography

17. Another big danger to children is posed by online pornography, to which many of them are being exposed at an early age. Although we do not have exact data for Hong Kong, the Children's Commissioner for England has reported that the majority of children are exposed to pornography by their early teens. Adult material is easily accessible, and its availability must be more strictly controlled. Children view online pornography for various reasons, and it can sometimes result in psychological damage. Sometimes children look at it out of curiosity, or else through inadvertence, but also sometimes as a result of peer pressure. Although Hong Kong has yet to take action to prevent this, how other jurisdictions deal with the problem could be studied.
18. In the United Kingdom, for example, the recently enacted Digital Economy Act, which has yet to come into force, requires all adult internet users wanting to view legal pornography online to prove that they are aged 18 or over by providing some form of identification, and there are criminal sanctions if online providers do not police age-verification techniques properly. Responsibility for checking ages has been given to private companies, and they are supervised by a regulator. Hong Kong also needs legislation of this type, particularly to protect young children from accidentally coming across pornographic material while they are browsing the internet, as many of them do these days.

Cyberbullying

19. In the United States, cyberbullying has been defined as "the use of any electronic communication device to harass, intimidate or bully" (State of Oregon).
20. In Hong Kong, cyberbullying is also a significant problem, involving the unauthorized use of a child's personal data online. Recent research by the Polytechnic University of Hong Kong showed that 54% of the 2,120 pupils surveyed had seen their personal information posted online without their consent, causing them depression, anxiety and stress. There has also been a huge increase in cyberbullying complaints, although many cases go unreported. Cyberbullying can cause just as much damage as actual physical bullying, and can even include mocking in social media exchanges. A dedicated law is therefore required to combat cyberbullying, and various models exist around the world, which could be adapted for use in Hong Kong.
21. In 2013, for example, South Africa enacted its Harmful Digital Communications Bill, to protect victims of "harmful digital communications", including text messages, pictures and other electronic communications. A perpetrator may be prosecuted if his actions have caused serious emotional distress to the victim. In 2014, Canada enacted its Protecting Canadians from Online Crime Act, which gave the police powers to investigate cyberbullying cases, to track perpetrators, and to seize electrical equipment used for cyberbullying activity. However, in the Asia-Pacific Region, the New Zealand response has been particularly impressive.

22. In 2015, New Zealand enacted its Harmful Digital Communications Act (HDCA), and this provides a useful model for others to follow. Its purpose is to "deter, prevent, and mitigate harm caused to individuals by digital communications", and to "provide victims of harmful digital communications with a quick and efficient means of redress". It seeks to curb cyberbullying which occurs through damaging electronic communications, whether by means of emails, texts or social media posts. The HDCA:
    a. Establishes an agency to efficiently resolve victims' complaints;
    b. Provides online content hosts with a process for handling victims' complaints;
    c. Gives the courts the power to issue take-down notices and impose penalties;
    d. Creates a new offence of sending messages and posting material online that deliberately causes serious emotional distress;
    e. Creates an offence of incitement to suicide even where the victim does not attempt to end his life.
23. As a result, businesses in New Zealand which host sites where posts can be placed must know how to deal with objectionable posts. An objectionable post is defined as one which discloses sensitive personal facts about somebody, or is intimidating, or is grossly offensive to an individual, or can be used to harass somebody, or contains a false allegation, or is indecent or obscene, or which incites people to send a message to an individual for the purpose of causing harm, or incites an individual to commit suicide, or unfairly denigrates an individual because of his color, race, religion, gender, or disability.
24. If an online content host receives a complaint about a post's content, they must notify its author and seek a response. If the author consents (or does not respond within 48 hours), the host may remove the content complained of. If, however, the author objects, the post cannot be removed, and the complainant must be notified. The complainant can then apply to a court for redress, including the removal of the post, the publishing of a correction or apology, or an order requiring an online content host to prevent access to a post, or else to provide information about the author to the court. If there is non-compliance, fines will be imposed.

Resolutions

25. ACA has urged the government to implement the following for years.
    a. The existing school sex education guideline was published by the Education Department in 1997. It's outdated and not in line with the developmental needs of children. It should be **reviewed and revised** in accordance with the psychosexual development and needs of children nowadays.
    b. Comprehensive and systematic sex education in schools should be implemented. Referring to some surveys, some schools spent little time, one to two hour(s) on sex education in a year which is inadequate for the growth and development of children. As sex education is actually life education and children need to acquire age appropriate knowledge and skills to meet their developmental needs, we recommend that sex education becomes **compulsory curriculum in schools**.

c. Allocation of resources for **professional training** (teacher and social worker), training materials and publicity events in the community is crucial.

26. Sexual exploitation online, sexual grooming, online pornography, and cyberbullying are posing danger to children. We suggest the cybercrime subcommittee to consider having these in its agenda.
27. Revised approaches to cybercrime, particularly if it targets children, are necessary, and this involves innovative thinking. Far more needs to be done to protect the victims.
28. **New laws** must be both comprehensive and futuristic.
29. **Regulations for internet providers** should be considered by the government requiring surveillance system over internet platforms on cyber safety, especially on sexual exploitation, sexual glooming, promotion of violence, use of threats, bullying, messages with deviant connotations, glorification of self-harm or suicidal behaviors, either pictorial or in descriptions by any other means.
30. **Law enforcers** must be given the tools to combat digital age dangers, and artificial intelligence has a vital role, particularly in identifying exploitative materials on websites.
31. Where, moreover, fraudulent internet platforms take advantage of jobseekers, they must be exposed. This requires better **regulation by technology companies**, as well as clear guidelines from **governmental employment agencies** explaining how jobseekers should protect themselves online. There are roles for both the public and private sectors, and these must be complementary, as they must pull in the same direction.
32. If cybercrime is to be combated, there must be improved cyber security, increased protection for children and other vulnerable persons, globally recognized standards and best practices, **coordinated** law enforcement operations in cyberspace, greater collaboration between government and civil society, and improved modes of international cooperation.