



Cyber-bullying – What you need to know

Introduction

The proliferation of communication technologies has transformed our lives. People are connected all the time by a variety of electronic means and devices. Through instant messaging services and social media accounts, people can share their daily life experiences and interact with friends and family, thereby sharing ideas, building relationships and having fun. Online, a person can access information shared by others with little or no restriction.

In many ways these technological innovations have made human interactions more efficient and more creative. However, increased connectivity leads to problems when strangers, critics, bystanders or even friends interact irresponsibly and without due regard to people's right to privacy. People's lives offline may be adversely affected as a result. One notable example of such unfortunate consequences is cyber-bullying.

Different forms of cyber-bullying

Cyber-bullying generally refers to bullying that involves the use of email, images or text messages sent to web pages, blogs, chat rooms, discussion forums, online gaming network, mobile phones, or other information and communication technology platforms. Behaviour of cyber-bullying includes harassment, denigration, disclosure of real-world identities, framing, impersonation, trickery and exclusion. Children as well as adults can be the victims of cyber-bullying. Whatever the mode, cyber-bullying can cause great distress to the victim and in the extreme cases lead to the most tragic of consequences: suicide.

Like their counterparts in the physical world, cyber-bullies sometimes try to persuade or bully other people into joining in with the abuse. The difference is that cyber-bullies are able to hide their identities on the Internet and they require neither the physical nor social prowess that may be needed for traditional bullying. Instead, online communication technology allows for continuous onslaught unrestrained by physical boundary. It is usually difficult to effectively stop cyber-bullying.

Risks in sharing information online

The unfortunate reality is that people give out far too much information about themselves online, with the erroneous belief that their information is private and they are safe behind the screen. The following risks may not be readily apparent to them.

- There is no simple "Delete" button to delete the information disclosed online. Though you may regret making an off the cuff remark on the Internet and delete it within an hour of posting, by then, to your dismay, it may have been read and forwarded to a great many other people.

Example 1:

A bride-to-be passed remarks on a social networking site, expressing her dissatisfaction with the wedding presents received. Shortly afterwards, users of various Internet forums criticised her attitude, and her wedding date and venue were made public. She was put under tremendous pressure and had to apologise in public.

- You may have thought twice before posting any message, information or photo, and limited access to “friends” only, but you have no control over what others share online. Your friends may not seek your permission or even inform you before re-posting your messages on their accounts or sites.

Example 2:

A girl posted a message to her friends online complaining that she had been dumped by her boyfriend. She accused her ex-boyfriend to have injured her by pushing her down a staircase. As a result, her “friends”, in cyber space parlance, showed their support by displaying the personal data of her ex-boyfriend including his name, photo and residential address on their sites. The “accused” sought relief by skipping classes for days and clarifying in a radio programme that the allegation was made with no factual basis. Some netizens avenged in the name of her ex-boyfriend and posted the girl’s personal data online.

- Smartphones with Internet connection and high quality cameras have become accessible and affordable to the average consumer. Smartphone users often capture incidents that take place in public and publish the same online. If you are picked on for your uncivil behaviour or just for a practical joke, you may attract publicity on the Internet not always to your liking. Some Internet forums are well-known for their members’ prowess in uncovering the identity of the persons featured in the online video clips. Even if you and/or your friends have only left fragmented information about you on different sites, others can find ways to collate all information about you without your knowledge.

Example 3:

Two passengers on a bus quarrelled over a seat. The dispute was captured by another passenger with a smartphone camera who then shared it online. Internet users went on to disclose the names and phone numbers of the protagonists on the Internet after uncovering their identities, who as a result faced tremendous pressure. Criticisms of the two passengers’ behaviour swamped most online forums.

- What you say or share online can draw scrutiny beyond your expectation. The information you shared with others could be targeted by cyber-bullies naming and shaming individuals in the name of Internet justice. They put you on trial over your online words or behaviour and give their verdicts. It is not uncommon that an “attacker” may end up as a victim when the tide turns.

Example 4:

A grumpy customer posted a video to rally netizens’ opposition against a shop for its poor customer service. She expressed her anger at the shop with nasty words. To her surprise, netizens found her actions unreasonable and she became the target of attack. Her photo, home and office addresses were published on the Internet. A social network group was set up calling for her apology.

- Cyber-bullying may also occur when someone poses as the victim and uses the victim’s account to send out offensive, harassing, inappropriate messages or “hate” mail to friends and family on the “friend” list, thus misleading them to believe the communication was sent by the victim.

Example 5:

Soon after a love relationship began, the boy shared his social network account password with his girlfriend. To her disappointment, the girl found from the boy’s social network activity logs posts relating to his previous relationships which were unknown to her. The girl then impersonated the boy and sent harassing messages to his ex-girlfriends.

- Cyber-bullies may set up their victims by making them angry so that they respond with an irate or offensive remark. Once the victim so responds, the cyber-bully will click on the inappropriate content button on his social network or chat screen and notify the Online Service Provider (“OSP”) that there is objectionable content in the victim’s account.

Example 6:

A couple broke up. Both vented their anger at each other on an online forum. Both had their own supporters. Their offensive remarks were reported to the OSP by the opposing side as inappropriate, thus leading to termination of their accounts with the OSP.

- You may believe that you are safe from cyber-bullying because you have never disclosed your personal data or communicated with others on the Internet. However, as the Internet is so closely wired, any individual, Internet user or not, is vulnerable to irresponsible online behaviour.

Example 7:

A girl, who had no social network account, was falsely accused by her classmate of being involved in compensated dating. The rumour spread on an online forum. Some of the girl’s friends posted her photo and telephone number for “investigation”. As a result, the girl received thousands of nuisance calls for sex service.

Legal protection

There is no statute law in Hong Kong on cyber-bullying. As such and in view of the fact that cyber-bullying activities are wide-ranging and cover defamation, criminal intimidation and infringement of intellectual property, they have to be addressed by relying on different branches of the law. Various law enforcement bodies are involved.

Where cyber-bullying engages the collection and use of personal data, the requirements of the Data Protection Principles (“DPPs”) in the Personal Data (Privacy) Ordinance (“Ordinance”) are relevant. DPPs 1 and 3 are particularly important:

- DPP1 – This principle requires the data user to collect only the personal data for a purpose directly related to its function or activity; collect data as necessary and not excessively; and collect data by means which are lawful and fair.

For instance, collection of personal data for the purpose of criminal intimidation is not for a lawful purpose and is therefore prohibited under DPP1.

- DPP3 – This principle stipulates that unless the data subject has given explicit and voluntary consent, personal data shall only be used for the purpose for which it was originally collected or a directly related purpose.

There is no exemption from DPP3 for personal data obtained from the public domain through channels such as public registers, search engines or public directories. In other words, cyber-bullying based on the use of personal data of targeted persons collected from these public sources is more than likely a contravention of DPP3.

The fact that an individual's personal data can be obtained from the public domain must not be taken to mean that the individual has given blanket consent for further use of his personal data for whatever purposes. Due regard must be given to (a) the original purpose of making the personal data available in the public domain, (b) the restrictions, if any, imposed on further uses of the data and (c) the reasonable expectation of personal data privacy of the individual. The legitimate expectation of privacy can be ascertained by asking whether a reasonable person in the shoes of the individual concerned would find the re-use of the data unexpected, inappropriate or otherwise objectionable, taking into account all factors in the circumstances. It is unlikely that a victim of cyber-bullying would accept that his personal data found in the public domain can be used to his detriment.

More detailed explanations on how DPP3 governs the use of personal data in the public domain are found in the Privacy Commissioner's *"Guidance on the Use of Personal Data Obtained from the Public Domain"*¹.

DPPs 1 and 3 may be exempted under section 52 of the Ordinance where personal data is held by an individual and is (a) concerned only with the management of his personal, family or household affairs; or (b) so held only for recreational purposes.

Contravention of a DPP per se is not an offence. In the circumstances, the Privacy Commissioner may serve an enforcement notice on the data user concerned to remedy the contravention and it is an offence for the data user not to comply with the enforcement notice. The offence attracts a fine of \$50,000 and imprisonment for two years and, in the case of a continuing offence, a daily fine of \$1,000.

Personal data protection

To curb cyber-bullying, users of social media networks are strongly advised to take steps to protect themselves. Their special attention is drawn to the following:

- What goes online stays online. Hence do not post any information online that you would not share publicly offline. Always assume that your "private" conversations will be published and become known one day, either by mistake or through the acts of your "friends".
- Posting comments or sending messages impulsively (e.g. when you are angry) are often regretted subsequently.
- Think twice before joining a heated discussion. Treat others the way you would like to be treated. You could be the next victim!
- Children may not understand the long-term implications of posting silly or offensive remarks or pictures. They may not appreciate it is not acceptable to harass, spread gossip, or make mean or disparaging comments towards others online. Parents need to educate children about their rights and responsibilities as netizens.
- Children should be taught to seek help from parents, teachers or adults that they can trust.

For tips on how to protect privacy when using social network platforms, please refer to the Privacy Commissioner's leaflet entitled *"Protecting Online Privacy – Be Smart on Social Networks"*².

¹ www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf

² www.pcpd.org.hk/english/publications/files/SN_e.pdf

Staying in control

If you believe that you are the victim of someone's online activity that is abusive or malicious, there are a number of things you can do:

- Children should seek help from parents, teachers or adults that they can trust. They should not shy away from showing to adults they can trust any messages that include threatening or harassing statements.
- For minor incidents of cyber-bullying, e.g. a mean or nasty comment, the best response could be no response.
- If the messages continue and you decide that the best strategy is to isolate yourself from the messages, you may use the social network sites' blocking feature to stop receiving the bullying messages. Most social networking sites as well as instant messaging programs have profile settings that allow a user to block other users from contacting them or showing comments on their accounts. [Note: Typically this option cannot stop bullies from continuing to post message and prevent others from seeing them.]
- Complain directly to the social network operator as abusive contents may be a violation of its acceptable use policy and subject to removal. Most social network sites have a link to their customer service department that allows individuals to report offensive messages, information or photos so that they can take action to remove them.
- If the posting carries criminal element e.g. criminal intimidation, or if it is indicative of a civil wrong, e.g. defamation or injurious falsehood, you may report to the Police or seek legal advice as to the appropriate recourse. If it is not known who sent or post the messages, the messages should be saved. They may provide trails to identify the perpetrator.
- If the cyber-bullying activities involve wrongful collection of personal data or misuse of personal data, a complaint may be lodged with the Office of the Privacy Commissioner for Personal Data. The complainant must be the person affected by the cyber-bullying or a person who has parental responsibility for the child who suffers from the cyber-bullying. To facilitate investigation into the complaint, the complainant must specify the identity of the bully by providing his name and contact details.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights

Reproduction of all or any parts of this leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer

The information provided in this leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

@ Office of the Privacy Commissioner for Personal Data, Hong Kong
First published in October 2014