Child's Play: Protecting the Privacy of Minors Online

What parent has not dealt with a huffy teenager demanding that parents "respect their privacy" and "keep out" of their room? Whilst children may be concerned about maintaining their privacy vis-a-vis their parents, their own increasing use of social media and voluntary disclosure of private information seems to send a conflicting message. The large number of photos, status updates, posts, etc., by the younger generation, seems to suggest a cavalier attitude to privacy and little or no concern about the potential implications of making such personal data publicly available. Has a teenager really thought carefully before he posted that photo of himself misbehaving during a night out drinking with friends? Has he really considered the future implications of a photo being spotted by a future employer or university admissions officer?

In May 2015, the Hong Kong Privacy Commissioner (**PC**) announced the results of a study carried out in October 2014, which revealed that children are now going online at a much younger age than ever before. The study also revealed a fundamental lack of awareness of the serious risks that are posed to a child's data privacy in their online activities by children, parents and teachers alike.

Personal Data Online

Following an incident in May 2015, when a Hong Kong pro-government group was accused of posting a video online showing students supporting the proposed electoral reform package, without the students' consent, the PC turned his attention to the issue of the online protection of young people's personal data. The video was made as part of an application for a study tour to the USA. The students alleged that the pro-government group had assured them that the video would not be made public.

Complaints with regard to this incident were made to the PC who is currently considering whether or not to launch a formal investigation. In the meantime, the PC issued a media statement on 13 May 2015, reminding organisations of the need to comply with the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**) in the collection and use of personal data, including personal data of minors[1]. This includes taking all practicable steps, on or before the collection of the personal data, to notify the relevant data subjects (i.e., the children) of the purpose for which their data is being collected and the classes of persons to whom their data may be transferred[2], and not using the data for any other purpose, than the purpose for which it was collected, unless with the express prior consent of the data subject[3].

On 11 May 2015, the PC also announced that he had joined the Global Privacy Enforcement Network (along with 27 other data privacy enforcement authorities) to conduct a Privacy Sweep that would examine websites and mobile apps to determine whether or not there are any issues regarding the personal data of minors[4]. The Privacy Sweep took place between 11 to 15 May 2015, and the results will be announced later this year.

---

[1] https://www.pcpd.org.hk/english/news_events/media_statements/press_20150513.html
[2] Data Protection Principle 1 of the PDPO
[3] Data Protection Principle 3 of the PDPO
[4] https://www.pcpd.org.hk/english/news_events/media_statements/press_20150511.html

In addition to being the class of most active users of the Internet, mobile apps and social networks, the young generation is also seen as one of the most vulnerable groups of data subjects. It is very likely that the results of the Privacy Sweep will be combined with the issuance of guidelines on how to educate the public on the steps that need to be taken to protect the privacy of minors.

Responsibility of Schools and Other Organisations

Schools and other organisations need to be cautious when collecting and using the personal data of children. Their obligations under the PDPO apply equally to minors as they do to adults. Schools, in particular, should ensure they have in place internal guidelines and codes of practice consistent with the provision of the law on the collection, use and retention of their students' personal data (including any former students or student applicants) and their families.

When collecting personal data of youngsters, it is important to ensure (amongst other things) that:

a. the personal data collected is not excessive, and is needed for a purpose directly related to the data user's functions or activities;

b. the data subject must have been informed on or before personal data was collected, of the purpose for which their data will be used and to whom it may be transferred – the wording used in the notification should be tailored towards the age group of the data subjects, and should use simple language that is easy to understand;

c. the personal data is not kept longer than is necessary in order for the purpose in which it was collected; and

d. the personal data is securely stored and safeguarded from unauthorised access, loss or damage.

An area to which schools and other organisations should also pay particular attention, is their obligation to comply with data access requests under the PDPO. Under the PDPO, a data access request may be made on behalf of a minor by their parent or guardian[5]. However, steps must be taken to ensure that the person making the request is authorised to do so on behalf of the minor, e.g., evidence should be provided showing that the requestor is the parent of the minor. Even if it is established that the requestor is a "relevant person", i.e., a parent or guardian, this does not necessarily mean that the school or other organisation should automatically comply with the data access request. It should only comply with the request, if it is satisfied that such is made "on behalf of" the minor, and not for the parent or guardian's own purposes. The nature of the data being requested may in itself make it sufficiently clear that the request is not being made for the benefit of the minor. For example, if a parent issues a data access request to a school asking for the address of his/her child, this should raise alarm bells with the school, since the child would clearly already know his own address, and would not need to issue a data access request to the school to obtain it. Therefore, the logical conclusion would be that the parent is likely making the data access request to further his/her own interest (e.g., to discover the location of the child who he may be denied access to by the court). In such circumstances, it is better for the school to exercise caution and seek evidence and/or an explanation from the parent as to why they are making the data access request, and possibly talk to the other parent or guardian of the minor.

Conclusion

Particular caution needs to be taken when collecting personal data from minors, due to the vulnerable nature of the group. It is likely that the PC will decide to issue guidance notes or take enforcement action against data users, especially those that target youngsters (e.g., online gaming companies), following the announcement of the results of its Privacy Sweep later this year. Proactive steps should be taken by schools and other organisations to conduct an internal data privacy audit (including a review of their personal information collection statements, their data retention policies, etc.), to ensure compliance with the PDPO.

[5] Section 18(1) of the PDPO

Contact Us

For inquiries related to this Legal Update, please contact the following persons or your usual contact at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Karen H. F. Lee
Associate
T: +852 2843 4452
E: karen.hf.lee@mayerbrownjsm.com