MAYER·BROWN JSM

Legal Update
Hong Kong
10 December 2015

VTech Hack – Largest Cybersecurity Breach Affecting Children

On 14 November 2015, VTech Holdings Limited (VTech) was hacked, resulting in the personal data of about 6.4 million children and 4.9 million parents being compromised worldwide. Out of the more than 11 million people involved, 5 million of them had their data stolen. This is the largest cyber attack affecting children's data worldwide. Investigations in Hong Kong, the United States and Britain are currently underway.

Background

VTech is a leading electronic learning toys company, headquartered in Hong Kong, with offices in 11 countries (including Australia, China, Singapore, South Korea and Malaysia). VTech is currently listed on the Hong Kong Stock Exchange.

The hacker accessed VTech's customer database through its Learning Lodge app store (which allows customers to download apps, games, e-books and educational content onto their VTech products) and Kid Connect servers (which allows parents to communicate with their children via an app on the children's VTech tablet). The databases contain the name, birth date and gender of the children, and the name, email address, password, IP addresses, postal address and download history of the parents. No credit card data, bank account information or any identity card numbers were stored on the databases.

The affected customers are located across 16 different countries with the majority of those affected being in the United States. Other places include France, the United Kingdom, Germany, Canada, Hong Kong and Australia.

VTech has already taken steps to try and minimise any further damage by notifying all affected individuals, and temporarily suspending its Learning Lodge and Kit Connect Service in order to conduct a security assessment.

Both the Hong Kong Privacy Commissioner (PC) and the authorities in the United States have commenced investigations into the hack, to determine whether VTech infringed any relevant laws and, if so, what remedial action should be taken.

Hong Kong Investigation

The PC has commenced an investigation into VTech's practices in order to determine whether VTech failed to comply with its security obligations under the Hong Kong Personal Data (Privacy) Ordinance (PDPO), thereby enabling the cyber attack to occur. Under the PDPO, VTech (as a data user) is obligated to implement practical steps to safeguard the personal data held by it from any unauthorised or accidental access, processing, erasure, loss or use (Data Protection Principle 4).

If the PC finds that VTech has failed to comply with such security and safeguarding obligations, he may issue an enforcement notice against the company requiring it to carry out remedial action (e.g., requirements regarding further encryption and IT security, etc). If VTech fails to comply with the enforcement notice, then it will be guilty of an offence, which attracts a maximum fine of HK$50,000 and 2 years imprisonment. Higher penalties apply in the event of repeated infringements on the same facts and/or subsequent infringement of other enforcement notices.

In the United States, at least two states (Connecticut and Illinois) are planning to conduct investigations into the VTech breach. Britain's data privacy regulator has also announced that it will be conducting an investigation.

Data Breach Notification

In Hong Kong, data users are not obligated to inform the PC or any data subjects of any security or data

privacy breach, but such notification is strongly recommended by the PC where there is a real risk of harm to data subjects. In October 2015, only weeks before the VTech hack, the PC issued a new Guidance on Data Breach Handling and the Giving of Breach Notifications (Data Breach Guidance Note). In brief, upon the occurrence of a data breach, the Data Breach Guidance Note recommends that:

a. the data user should take immediate remedial action to minimise any harm or damage that could be caused to the data subjects;

b. the data user should promptly gather essential information on when the breach occurred; where it took place; how the breach was detected any by whom; the cause of the breach; the type and extent of personal data involved; and the number of data subjects affected;

c. the data user should designate an appropriate person or team to handle the data breach incident and coordinate the initial internal investigations into the breach;

d. the data user should identify the cause of the breach and take steps to stop/contain the breach, including stopping the relevant system if the breach is caused by system failure; changing the users' password and system configuration; notifying the relevant law enforcement agencies (e.g., the police) if identity theft, fraud or other crimes are likely to be committed; making the data processor take remedial steps if the breach is caused by the data processor, etc;

e. the data user should assess the risk of harm that could be caused by the data breach, e.g., identity theft, financial loss, damage to reputation, loss of dignity, loss of business, etc. The extent of such harm will depend on, for example, the type of personal data affected, the amount of personal data involved, the circumstances of the breach, whether the data was encrypted, etc;

f. if there is a real risk of harm (e.g., personal data stolen includes financial data, etc), then the data user should consider notifying the data subjects, the PC, law enforcement agencies and any other regulators or relevant parties (e.g., asking Internet forums to take down any leaked personal data that has been posted by hackers on the forum). The notification should be done as soon as possible, unless the law enforcement agency has (for investigative purposes) asked the data user to delay in notifying the data subjects. The Data Breach Guidance Note gives further details/ advice on what should be included in such notices (e.g., a description of what occurred, when it occurred, etc);

g. the data user should identify the root cause of the problem and take steps to prevent the recurrence of such a breach in the future, e.g., improving its security measures, limiting its employees' access rights to the personal data on a need-to-know basis, etc.

Whilst the Data Breach Guidance Note is not mandatory, and failure to comply with it does not in itself result in an offence, the PC will very likely take into account any failure to comply with the Data Breach Guidance Note in determining whether or not to issue an enforcement notice against the data user in the event of a breach.

Youth and Privacy in Hong Kong

The PDPO does not offer different treatment for minors' personal data. Minors' personal data is largely treated the same under the PDPO as personal data relating to adults. A few exceptions apply in respect to consent and the submission of data access and correction requests, some of which were introduced by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance 2012):

a. A parent or guardian are expressly allowed to make a data access request on behalf of minors. However, caution must be exercised by the data user 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. Further, data users should only comply with a data access request submitted by the parent or guardian, if the data user is satisfied that such is made "on behalf of" the minor, and not for the parent or guardian's own purposes.

b. With regard to consent, before the PDPO was amended in 2012, when a data user wanted to use the personal data of a minor for a new purpose, it had to obtain the "prescribed consent" of the data subject himself (i.e., the minor). There was previously no specific

provision in the PDPO that enabled a "relevant person" (i.e., parent or guardian) to give "prescribed consent" on behalf of the minor. Instead, Data Protection Principle (DPP) 3 required the prescribed consent to be given by the "data subject" themselves (i.e., the minor). However, changes were introduced by the Amendment Ordinance 2012 and the PDPO now expressly allows parents or guardians to provide prescribed consent on behalf of a minor in order for a data user to use the minor's personal data for a new purpose. Even after receiving such consent from a parent or guardian, DPP 3 still prevents the data user from using the data for the new purpose unless it reasonably believes that such new purpose is in the interests of the minor.

c. The Amendment Ordinance 2012 also introduced a new exemption to DPP 3 in the PDPO. Pursuant to the amendment, the police or the Customs and Excise Department may transfer any personal data of a minor held by them to the minor's parent or guardian (without needing any prior consent of the minor), if it is necessary to facilitate the better discharge of the parent or guardian's responsibility of exercising proper care and guardianship, and is in the best interests of the minor.

Ironically, the VTech hack occurred shortly after both the current and former PC raised concerns on the widespread collection and use of children's personal data. In May 2015, the former PC announced the results of a study carried out in October 2014, which revealed a fundamental lack of awareness of the serious risks posed to children's data privacy[1]. On 4 September 2015, the new PC announced the results of the Global Privacy Enforcement Network Privacy Sweep 2015 ("the Sweep"), which examined the website and mobile apps used by children[2]. The Sweep determined that of the 1,494 websites and apps examined:

a. 67% collected personal data of children, including name, birth date, contact number and address, and photos or videos;

b. 78% did not use simple language or provide warnings to children regarding the collection of their personal data, in a manner that could be easily read and understood by them;

c. 51% shared personal data with third parties, some of which were shared for vague or unspecified purposes;

d. only 24% encouraged children to involve their parents; and

e. only 31% had in place effective means of limiting the amount of personal data collected from children.

On 1 December 2015, following the VTech hack and the results of the Sweep, the PC issued a guidance note on the Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children (Guidance on Collection of Children's Data) and a leaflet entitled Children's Online Privacy – Practical Tips for Parents and Teachers (with advice on how parents and educators should get involved in children's online activities, etc).

The Guidance on Collection of Children's Data highlights the fact that children are a vulnerable group, and extra caution is required when handling their personal data. In brief, the Guidance on Collection of Children's Data recommends that:

a. data users not only limit the type and amount of personal data collected, but they should consider altogether avoiding the collection of children's personal data where possible;

b. children may not fully understand the privacy risks involved with oversharing and are generally more inclined to follow instructions. When minors' data is collected, data users should avoid adopting complex forms comprising both mandatory and non-mandatory fields. Instead, they should consider using a two-part form which clearly groups the mandatory fields and voluntary fields separately. The forms should also avoid using open questions, which risk the oversupply of information. Where children are asked to provide personal data about others (e.g., their parents or friends), they need to be warned to consult and obtain consent from such persons beforehand;

c. if the data user operates a discussion forum, they should ensure that children are notified

[1] See our article "*Child's Play: Protecting the Privacy of Minors Online*"
[2] "*Privacy Sweep Spots Concerns over Personal Data Collected by Websites and Apps Targeting Youngsters*"

beforehand of who can join the forums, who will have access to their posts, whether the forums are monitored or moderated by the data user, etc. Children should be able to preview their content before posting it, and should also be allowed to subsequently delete or edit their posts. Children should be reminded that even if they delete a post or restrict who can view their posts, other members can easily take a screenshot or otherwise copy and repost or distribute the content, which will be outside of the child's control;

d. data users should ask children to consult with their parents or teachers first before providing any personal data online;

e. data users should apply default settings to all children accounts on online platforms that allow the sharing of information, to ensure that the sharing of such data is as restricted as possible;

f. when a data user's online platform redirects children to other sites, the data user should ensure a clear notice is given to the children (i.e., by providing details of the redirected site and its relationship with the data user); and

g. age-appropriate language and presentation should be used for any personal information collection statement or privacy policy, to ensure that such documents can be easily understood by children.

Conclusion

Children spend a large portion of their time online - playing games, sharing photos, expressing opinions, chatting, etc. Do you, as a parent, know what your child is up to online? Children and parents may not even be aware of what data is actually being collected by various service operators. In this age of big data, a vast amount of information can be collected on a child, enabling data users to formulate a personal profile.

The VTech hack has highlighted the importance of protecting children's personal data, especially due to their vulnerability. Having in place robust security settings to protect personal data from being hacked will not be sufficient – it is also essential for data users to have in place internal practices specifically regarding the collection of children's personal data in general.

Whilst it is important to get children involved at an early age to help them understand their privacy rights, in reality (depending on the age group) it may not always be possible to rely on them to make fully-informed and thought-out decisions. Parents, educators and data users have an obligation to ensure that children's personal data is protected. Data users, in particular, should exercise a higher level of caution when collecting minors' personal data.

The more personal data collected, the broader the purposes of use and the greater the amount of people who can access the data, means a higher amount of risk. In this case, less is more. In the wake of the VTech hack, data users may wish to take a more restrictive approach when dealing with children's personal data.

Contact Us

For enquiries 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
Senior Associate
T: +852 2843 4452
E: karen.hf.lee@mayerbrownjsm.com