

Speech by SJ at plenary session of 16th China-ASEAN Prosecutors-General Conference in Brunei (English only)

Following is the speech by the Secretary for Justice, Mr Paul Lam, SC, at the plenary session of the 16th China-ASEAN Prosecutors-General Conference in Brunei today (October 22):

Your Excellencies, distinguished delegates, ladies and gentlemen,

Children today grow up in an interconnected digital world that offers unprecedented opportunities for education and development. But at the same time, modern technology exposes them to grave and fast-evolving risks - from violent or pornographic content on social media platforms, to online grooming, non-consensual sharing of intimate images, deepfake manipulation, cyberbullying, coercion and fraud.

The stark reality is that digital harm to children knows no borders. For example, an intimate image of a child, once created or uploaded, can be copied, disseminated and recirculated repeatedly and instantaneously across different jurisdictions. A child may have to live with the fear that such material will resurface at any time, transforming a single act of abuse into a cycle of victimisation. Against this backdrop, protecting children in the digital age is an urgent, shared regional and international responsibility which demands synchronised legal and institutional responses.

Hong Kong's existing legal framework

In this respect, Hong Kong maintains a solid legal framework to protect children from online sexual exploitation and other forms of cyber-enabled crime.

To begin with, the Prevention of Child Pornography Ordinance criminalises a broad range of conduct involving child pornography, including printing, producing, copying, importing, exporting, publishing, and possessing child pornography, with maximum penalties ranging from three to eight years' imprisonment upon conviction. The Ordinance includes express provisions for the forfeiture of any child pornography, as well as any machinery or apparatus used to commit the relevant offences.

Importantly, the statutory definition of "child pornography" under the Ordinance encompasses any "computer-generated image or other visual depiction" - irrespective of whether it is generated by electronic or other means, whether it depicts a real person, or whether it has been "modified". The Ordinance thus extends beyond traditional physical media to capture synthetic, computer-generated, or altered materials. This statutory definition is vital in ensuring that our legal framework remains future-proofed against rapid technological change.

Another milestone in Hong Kong's legislative framework is the enactment of the comprehensive voyeurism and non-consensual intimate image regime under Part XIIIA

of the Crimes Ordinance in 2021. Voyeurism covers acts of observing or recording, with or without equipment, another person's intimate part or doing an intimate act without consent for the purpose of obtaining sexual gratification or causing humiliation, distress, or alarm. This law also criminalises acts of non-consensual recording, publication and threatened publication of intimate images, carrying maximum penalties up to five years' imprisonment. "Intimate image" under the Ordinance includes an image that has been altered to appear to show an intimate part or an individual doing an intimate act, providing a clear legal basis to tackle digital editing and manipulation - tactics increasingly used for online extortion and sexual exploitation.

Significantly, the legislation provides that a child under 16 is legally incapable of giving consent. This provides vital protection for young people vulnerable to online image exploitation.

Furthermore, the statutory framework empowers our courts to issue a disposal order requiring any person, whether in Hong Kong and elsewhere, to take reasonable steps to remove, delete, or destroy such images, at any stage during criminal proceedings, and its validity remains unaffected even if the prosecution is subsequently discontinued or the defendant is acquitted. Importantly, the court can order the service of such disposal order on a person or entity out of jurisdiction. This extra-territorial mechanism applies to online platforms and social media providers operating outside Hong Kong, ensuring that our laws do not merely punish offenders but actively disrupt the cycle of victimisation at its source.

The above statutes are examples of Hong Kong's legislation tailored specifically to child protection. But it must be borne in mind that many traditional criminal offences are "technologically neutral" - meaning that the law applies with equal force regardless of whether the offence is committed physically or via digital means. For instance, cyberbullying or online extortion may be prosecuted under offences such as criminal intimidation, carrying a maximum penalty of five years' imprisonment, or blackmail with a maximum penalty of 14 years' imprisonment. In a Court of Appeal case decided back in 2018, the defendant who secretly recorded intimate videos of his partner and threatened their online dissemination to her colleagues and friends was convicted for, among other things, the offence of criminal intimidation. The Court laid down key sentencing principles for secret filming - specifically recognising the grave risk of rapid, indefinite online spread.

Child protection as a shared responsibility

Having said all these, we recognise that maintaining existing a legal framework alone is not enough. As the Court of Appeal highlighted in the recent case decided earlier this year, young and inexperienced users are increasingly vulnerable to being lured into harm through online dating and networking platforms.

In that case, a 16-year-old girl was lured via a dating app by a 41-year-old man posing as a 27 year old, leading to sexual abuse and rape. The Court of Appeal remarked that

owners and operators of social media, dating applications, and other online platforms cannot treat criminal conduct on their services as a matter solely for law enforcement. Rather, platform providers play a pivotal role in shaping a safe online environment.

This case serves as an important reminder that child protection in the digital age is a shared responsibility that cannot rely solely on criminal prosecution. Safeguarding children from modern virtual risks requires a co-ordinated strategy combining effective legislation, rigorous law enforcement, industry accountability, early intervention, and public education.

Hong Kong's responses to emerging risks

In response to the growing need to protect children amidst rapid technological change, Hong Kong has advanced a series of key initiatives for better protection of children.

As a broader strategic background, Hong Kong published its First Five-Year Plan for Economic and Social Development (First Five-Year Plan for Economic and Social Development of the Hong Kong Special Administrative Region (2026-2030)) on September 16, 2026, in alignment with the National 15th Five-Year Plan. The Plan sets down long-term strategic directives to, among other key areas, fortify security governance, combat newly emerged cybercrimes through deeper cross-boundary law enforcement collaboration, and enhance child welfare and abuse reporting mechanisms.

First, the Chief Executive of the Hong Kong Special Administrative Region (SAR) has announced in the Policy Address 2026 that a dedicated task force on minors' use of social media will be established under the Inter-Departmental Working Group to Review Legislation to Support Wider Application of AI spearheaded by the Department of Justice. The task force will review the risks associated with the use of social media by minors, and assess the need for more targeted legislative and administrative solutions.

In considering the way forward, the Government will study international regulatory models and explore measures suitable for Hong Kong, particularly regarding the responsibilities of Internet service providers. For instance:

- (1) whether the platforms should be required to systematically identify risk of criminal conduct on their services and implement effective user warnings;
- (2) whether heightened protective measures and age-related safeguards should be mandated for minor users;
- (3) whether the platforms should maintain simple, accessible reporting mechanisms for suspicious or abusive behaviour that trigger transparent, effective responses, including timely co-operation with law enforcement agencies.

The purpose of this initiative is not to isolate children from technology, nor to restrict their digital participation and fundamental rights. Rather, it is to ensure that children will not be exposed to risks and can engage with the online world safely, with appropriate safeguards against misinformation, harmful materials, or even illegal content.

Of course, legislative intervention is one among many tools. We need hard law on the one hand and soft mechanisms - such as industry guidelines, codes of conduct, and public education - on the other to drive proactive compliance. These tools are not mutually exclusive; they should operate in parallel. To this end, as also announced in the Policy Address 2026, the Education Bureau of the Hong Kong SAR will support schools in guiding students to use AI tools prudently, equipping them with the digital literacy and values needed to navigate online risks.

Second, also under the strategic directions of the Five-Year Plan and the Policy Address 2026, the Cybercrime Sub-committee of the Law Reform Commission is conducting an in-depth review of our legal framework, focusing specifically on AI-enabled crimes, including those targeting children. Having published its first report recommending bespoke cybercrime legislation, the Sub-committee's ongoing work centres on formulating robust statutory measures to tackle the illicit production of synthetic pornographic images, online fraud, and deepfake exploitation directed at minors.

Third, the Hong Kong SAR Government will introduce an amendment bill to comprehensively reform our sexual offence regime. This includes eight new bespoke child sexual offences, such as grooming, causing a child to view sexual images, and engaging in sexual communication with a child. These targeted proposals address modern online harms, from cyberflashing, online sexual exploitation, to digital sex trafficking.

Fourth, the Department of Justice has established a dedicated task force on vulnerable witnesses and child protection. Bringing together its Prosecutions Division, the Hong Kong Police Force, and the Social Welfare Department, this specialised task force fosters seamless multi-agency collaboration - facilitating early prosecutor intervention, expedited legal advice, and tailored court safeguards to minimise trauma for child victims throughout the judicial process. Under this joint framework, this task force has issued around 900 pieces of advice since its inception in 2022.

Fifth, given the transnational nature of online child sexual exploitation, the Hong Kong Police Force has actively deepened international co-operation. In 2025, the Force joined the International Child Sexual Exploitation database of the INTERPOL (International Criminal Police Organization), an intelligence and investigative platform through which specialised investigators utilise advanced algorithms and intelligence sharing across more than 70 jurisdictions to identify victims and offenders.

In addition, the Police Force regularly participates in joint multi-jurisdictional operations. Notably, from March to April this year, Hong Kong joined law enforcement agencies from Brunei, Singapore, Malaysia, Japan, South Korea, and Thailand in a co-ordinated operation against child pornography, resulting in 326 arrests and the seizure of various mobile devices containing child pornographic materials.

The need for international co-operation

As I mentioned at the outset, cybercrimes targeted at children know no jurisdictional limits. Cross-border co-operation is indispensable. In this regard, I wish to highlight four essential areas for our joint collaborative efforts in child protection in the modern technological era.

First, keeping our legal frameworks abreast of technological change requires sharing of knowledge and experience. As cyber threats rapidly evolve, no single jurisdiction has all the answers. By sharing regulatory approaches and law drafting experiences, we can refine and update our existing laws.

Wherever appropriate, legislation should be designed with extra-territorial application. This is essential to enable effective investigation and prosecution when offenders operate in one country, target children in another, and disseminate abusive material across platforms hosted in a third.

Secondly, effective mutual legal assistance arrangements and adaptable evidence rules are essential for prosecuting transnational crimes where overseas evidence and child witnesses are involved. In Hong Kong, under Part IIIA of the Criminal Procedure Ordinance, child witnesses who may not be able to endure the pressure of testifying in a traditional courtroom are permitted to give evidence via a live video-link or through pre-recorded interviews. Further, under Part VIIIA of the Evidence Ordinance, our courts may issue letters of request to foreign authorities to obtain evidence out of the jurisdiction, which is a very useful tool to obtain evidence in transboundary crimes.

In addition, relaxing the exceptions to the criminal hearsay rule under the common law is necessary to enable that the admissibility of foreign digital logs, records, and out-of-court statements in criminal proceedings. In this regard, Hong Kong is introducing a major reform of the hearsay rule in criminal and surrender proceedings under the Evidence (Amendment) Bill 2026 which was gazetted on June 12, 2026.

Thirdly, priority should be given to deepening co-operation between law enforcement agencies worldwide. As the Hong Kong experience shows, co-ordinated action can produce fruitful and meaningful results.

Our respective law enforcement agencies should establish clear and accessible communication channels with each other so as to facilitate the timely exchange of information and intelligence. Information shared promptly may enable authorities to identify children at immediate risk, locate offenders, or prevent the circulation of harmful material. By maintaining regular liaison at both the strategic and operational levels, we can significantly improve our ability to identify offenders of cross-border cybercrime and child exploitation early, and take prompt intervention action to disrupt cybercrime networks.

Lastly, we should not lose sight of the importance of continuous training and professional development of officers involved in the protection of children against

transnational cybercrime. Specialist training is critical to protecting children in the digital age. Law enforcement agencies and other professionals working in this area must be well equipped to recognise the indicators of online grooming, AI-facilitated exploitation, and child abuse activities in various forms and manifestations. To this extent, regular international conferences and symposiums, meetings and working groups, as well as training courses, workshops, and seminars have an important role to play in cultivating our professional expertise. If cybercriminals can adapt and learn quickly from one another, we must be able to do better.

Conclusion

Your Excellencies, distinguished delegates, ladies and gentlemen. It is often said that children are the future of the world. As prosecutors and ministers of justice representing our communities, it is incumbent upon us to ensure that children in this day and age can grow, learn, and explore in the digital world without being exposed to exploitation, abuse, or manipulation. That can only be done if governments join hands to take effective measures locally, regionally, and globally, to strengthen co-operation at all levels and among all relevant agencies. As I have said before, "alone we can do so little, together we can do so much". On behalf of the Hong Kong SAR, I can say loud and clear that all branches of our Government will continue to promote international co-operation to better the protection for children amidst the digital age in all ways possible.

On this note, may I once conclude by congratulating the Attorney General's Chambers of Brunei Darussalam for holding this important and successful conference, and expressing our utmost gratitude to your warm hospitality. My gratitude also goes to all the distinguished speakers for sharing their invaluable insights and experience. Thank you very much.

Ends/Thursday, October 22, 2026