Hong Kong

Michelle Ta has a breadth of experience across technology transactions, IT outsourcing, software and IP licensing, and privacy and data protection, and she has also made achievements in the field of financial technology. She has provided a series of data-related consulting services for virtual banks and fintech clients, and is currently seconded part-time to a virtual bank in Hong Kong to provide long-term legal support. Michelle is also an experienced cybersecurity legal advisor, and has acted in-house for a global IT services giant as the company's cybersecurity subject matter expert.

Clients have described Michelle as 'one of the few lawyers I would call having the full package', 'a lawyer to watch out for in the TMT sector' and having 'excellent technical skills and great commercial judgment across banking, technology and corporate practice'. Michelle was recognised for her commercial acumen as a finalist for the prestigious Australian Financial Review BOSS Young Executive of the Year award in 2017.

Michelle is dual-qualified in Hong Kong SAR and Victoria, Australia. She graduated from the University of Melbourne with first class honours in Law and holds a second bachelor degree in science, with double majors in biochemistry and biotechnology.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Hong Kong does not have a dedicated cybersecurity statute or mandated cybersecurity standards. However, there are a variety of sector-specific requirements for regulated businesses and cybersecurity continues to be an area of intense focus for financial regulators such as the Hong Kong Securities and Futures Commission (SFC) and Hong Kong Monetary Authority (HKMA).

For example, at the start of 2021, the HKMA implemented an upgraded Cybersecurity Fortification Initiative (CFI 2.0). The original CFI regime was launched in 2016, and CFI 2.0 is a result of the HKMA's recognition that cybersecurity is a rapidly evolving landscape. The CFI contains enhanced expectations of attack simulation testing, cyberattack readiness and cyber resilience controls. This is a continuation of the HKMA's long-held focus on protecting customer data, which continues to be a major area of focus as banks increasingly become more digital.

The SFC has also been working to bolster its cybersecurity expectations. In 2020, it issued a thematic cybersecurity review of internet brokerages, which indicate the SFC's continuing concerns that mobile applications and other digital interfaces are more vulnerable to hacking risks and security breaches than traditional forms of interfacing with clients. The SFC has called out encryption, user access management and tracking of data access as particular areas of focus (and this is also consistent with the focus of parts of the SFC's introduction of more stringent cloud storage requirements over the past couple of years). More recently, the SFC has also used further guidance on managing the cybersecurity risks of remote working.

In terms of legal changes, the last major change occurred in 2019. Hong Kong has traditionally leveraged section 161 of the Crimes Ordinance to tackle cybercrime. Section 161 of the Crimes Ordinance deals with access to a computer with a criminal or dishonest intent, for example, with intent to commit an offence, with a dishonest intent to deceive, with a view to dishonest gain, or with a dishonest intent to cause loss to another.

Section 161 – typically understood as a hacking offence – has been used in Hong Kong over the years as a 'catch-all' offence for all manner of crimes committed using computer devices, including things like 'upskirting' (taking sexually intrusive photos so as to see up a person's skirt or dress without permission). This changed in 2019 when a Court of Final Appeal judgment (*Secretary for Justice v. Cheng Ka Yee*) confirmed that section 161 does not apply to a person's use of his or her own computer. This judgment has redefined section 161 as a provision aimed at tackling cybercrime.


Michelle Ta

While section 161 of the Crimes Ordinance currently still remains the only 'per se' cybercrime statutory provision in Hong Kong, in October 2021, the Hong Kong government announced plans to implement a new cybersecurity law to help ensure the security of Hong Kong's network information systems at a macro level, which is expected to cover important or critical infrastructure, such as government agencies, financial institutions, telecommunications facilities and public transportation facilities. The Security Bureau, being the relevant governmental department taking the lead on this, is expected to submit documents to the Hong Kong legislative council as well as launch public consultations by the end of this year, and the government has expressed that references will be drawn from cybersecurity standards adopted worldwide in formulating relevant standards in Hong Kong.

Additionally, an amendment to the Personal Data (Privacy) Ordinance (PDPO) in Hong Kong took effect on 8 October 2021 to prevent a type of cyber offence known as 'doxxing', which is the publishing of personal identifying data without consent with malicious intent. The amendments made to the PDPO seek to close a policy loophole by giving the Privacy Commissioner for Personal Data (PCPD) greater enforcement powers including powers to institute prosecutions and order the

removal of doxxing content. It has particular implications for insider threats and 'stray employee' cybersecurity risks, and for companies that allow user-generated content like social media platforms. The new anti-doxxing provisions also come with extraterritorial effect, where section 66M(2) of the PDPO now gives the PCPD power to direct a service provider, whether it is in Hong Kong or not, to take certain actions (including taking down content) in cases of doxxing. Companies (and in particular those in the TMT sector) should continue to look at and bolster external policies on platform use and internal policies on the handling of personal data and content moderation, such as developing and investing in measures to curb doxxing or provide training on how to respond to cessation notices.

Finally, the PCPD recently issued a new Guidance Note on the Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data, in which two new sets of recommended model contractual clauses (RMCs) are introduced, namely data-user-to-data user RMCs and data-user-to-data-processor RMCs. The data-user-to-data-user RMCs set out model clauses for data transfers between two data users (or data controllers) and are aimed at ensuring that a transferor takes all reasonable precautions to ensure that personal data transferred to a transferee acting in the capacity as a data user is not processed in a manner that would violate the PDPO. The data-user-to-data-processor RMCs sets out model clauses reflecting the PDPO requirement that a data user remains accountable for the acts of its data processors and imposes contractual obligations to oblige data processor transferees to comply with the requirements of the PDPO. The RMCs are recommended by the PCPD to be incorporated in agreements where personal data may be transferred outside of Hong Kong by a local entity to an overseas entity, or between two entities outside of Hong Kong where such transfer is controlled by a data user that is subject to the PDPO.

In reality, the RMCs are difficult to implement and are likely to be resisted by data processors, because they comprise certain obligations that lie beyond the control of data processors, such as requiring the transferee to ensure personal data transferred is adequate but not excessive. The actual law itself has not changed (and in particular, the relevant section of the PDPO (section 33) restricting cross-border transfer of data is still yet to come into effect with no timetable announced for its implementation). Adoption of the RMCs is therefore not mandatory. Organisations are also free to adapt and modify the RMCs or use alternative wording as long as they are consistent with PDPO requirements. As such, the RMCs are likely to be negotiated heavily by both data users and data processors, and we do not expect the same level of widespread use as that seen, for example, with the Standard Contractual Clauses under the GDPR.

"The Hong Kong government has been discussing a range of changes to the Hong Kong privacy law, including introducing a mandatory data breach notification regime."

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

There is no general mandatory data breach reporting regime in Hong Kong. While reporting of data breaches is encouraged by the Hong Kong Privacy Commissioner, as a matter of practice, we see clients take a range of approaches to voluntary reporting (whether that is reporting to the regulator or affected consumers). Usually the things that clients weigh up include whether the data breach might have to be reported on a mandatory basis in another jurisdiction (in which case, clients tend to lean to voluntary reporting in other affected jurisdictions); the size of the data breach; and the risk of harm to affected individuals. Factors such as negative public perception and financial consequences are also important considerations.

That said, since the start of 2020, the Hong Kong government has been discussing a range of changes to the Hong Kong privacy law, including introducing a mandatory data breach notification regime. While we are yet to see legislative progress regarding a mandatory data breach notification regime, we expect this to

stay high on the agenda in Hong Kong and that it will become law in the not-too-distant future.

Of course, for regulated businesses – and in particular, those businesses that are subject to the supervision of financial regulators – there continue to be sector-specific regulatory expectations to report data incidents within certain time frames.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The biggest issues that companies need to consider from a privacy perspective arise even before companies suffer a data security incident.

First of all, data security (and privacy protection in particular) should be board-level issues. Too often, they are considered the sole domain of certain stakeholders (the CISO, a data protection officer or another 'tech' or 'legal' person) – so the first issue that companies need to address from a privacy perspective is an understanding that this is an enterprise-wide responsibility.

Photo: shutterstock/ESBProfessional

Dealing well with a data security incident starts from prevention in the first place, followed by good preparation for the worst-case scenario. The companies that do this best have a multidisciplinary team (stakeholders from senior management through to lawyers, public and government relations experts, cyber forensics professionals) that have been trained and drilled for cyber incident simulations so that they can mobilise quickly to respond to a data security incident when it (inevitably) occurs. Those companies know what steps they need to take and the order in which they need to take those steps – from initial containment of a data breach, through to ensuring key evidence is collected in a way that maintains chain-of-custody (particularly important so that digital evidence is not accidentally erased or changed in an effort to fix a breach), through to taking measures to fix vulnerabilities and post-mortem reviews. All of that will be important if a company is required to report an incident to a specific regulator (for example, the HKMA) or if the company decides it wants to voluntarily report the incident to the Privacy Commissioner or affected customers.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

There are a range of approaches in Hong Kong to cybersecurity preparedness. Banks are among those that have the highest level of regulatory expectations when it comes to cybersecurity preparedness and cyber resilience. In terms of best practice, regulated banks in Hong Kong must meet a minimum baseline of cybersecurity readiness, which is set out in the HKMA's Cybersecurity Fortification Initiative. This comprises three pillars – the Cyber Resilience Assessment Framework, which helps banks assess their cyber risk posture and benchmark their level of defence and resilience; the Professional Development Programme, which is a certification scheme for cybersecurity practitioners in the industry to boost technical capability in areas such as attack simulation testing; and the Cyber Intelligence Sharing Platform, which is aimed at sharing cyberthreat intelligence to help the industry stay informed of, and prepare for, emerging hacking tactics and patterns.

This is consistent with common cybersecurity wisdom that cybersecurity is a patchwork of defences in an organisation's people, processes and technology.

Other sectors take a range of approaches to cybersecurity preparedness, and there remains a broad spectrum of cybersecurity maturity levels in Hong Kong.

"Organisations that are supervised by the SFC in Hong Kong should be particularly aware of additional requirements imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records."

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Yes – in particular organisations that are supervised by the SFC in Hong Kong should be particularly aware of additional requirements imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records. The SFC issued a Circular in late 2019, and in late 2020 a set of accompanying FAQs, setting out certain requirements for licensed corporations wishing to move their data storage to a cloud hosted environment. Some of the requirements and expectations set out in this regime impose sector-specific requirements which are unusual both in the context of cloud service agreements in a broader sector-agnostic context as well as in comparison to expectations in the same sector in other jurisdictions, including, for example, a requirement to maintain a full and immutable audit trail to memorialise access logs by every unique user of a data record.

Outside of these requirements of the SFC, there are of course all the usual requirements that businesses should consider when thinking about moving data

to an environment hosted by a third party – including due diligence to ensure the relevant cloud product is fit for the intended purpose, that the vendor is certified against prevailing industry cybersecurity standards, that the vendor can meet required data availability and uptime commitments and that there is a certain level of redundancy and disaster recovery to protect data loss. In addition, cross-border data transfer restrictions are becoming more complex for projects for moving to a cloud hosted environment touching on multiple jurisdictions. Finally, increasingly, concerns about increased exposure to excessive government or regulatory access to cloud hosted data (and in some cases, conflict of law issues) are becoming a top consideration when looking to move data to the cloud.

6 | How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

A specialist unit within the Hong Kong Police – the Cyber Security and Technology Crime Bureau – is responsible for investigating and handling technology crime, computer examinations and preventing technology crime.

In addition, as discussed in further detail above in question 1, an amendment was passed last year to reform the Personal Data (Privacy) Ordinance to combat malicious doxxing acts and protect the public's personal privacy. A raft of new enforcement powers were also conferred on the PCPD to investigate and prosecute doxxing crimes, as well as granting the PCPD with the power to issue cessation notices with extraterritorial effect.

In relation to the proposed development of a local cybersecurity law, we expect to see documents submitted to the legislative council and public consultations launched in the second half of 2022, with the aim to enhance the cybersecurity of critical infrastructure in the city through legislation that will seek to require all private and public enterprises to comply with cybersecurity regulations.

7 | When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

All companies should be doing appropriate level of privacy and data security due diligence when looking at a potential acquisition or merger target. This involves diligence from a legal perspective (eg, whether there have been any recent mandatory or voluntary data breaches notified to regulators, whether there have been any near misses and whether there have been any data handling complaints or litigation that may indicate a systemic issue), as well as from a technical perspective (eg, bringing in cybersecurity professionals to assess a potential target's cybersecurity posture).

This is particularly important for companies that engage in businesses that are data-intensive, businesses that interface directly with consumers or businesses that are subject to particularly strict privacy laws in other jurisdictions. A history of multiple or serious non-compliances with the applicable data law, spotted during the due diligence process, may affect the value, terms or indeed continuation of the deal. These risks should also factor into decisions about M&A deal shapes and ways in which sellers may be required to remain financially responsible or accept more onerous terms for latent privacy and data security issues.

Michelle Ta
michelle.ta@simmons-simmons.com

Simmons & Simmons
Hong Kong
www.simmons-simmons.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Clients should also look for curious lawyers with an in-depth understanding of technology, computers and cybersecurity as a discipline (ie, knowledge beyond the strictly legal) with a good team of litigator colleagues working alongside them to cover tricky dealings with customers or regulators. It is important to look for a team with a good working knowledge of data law across multiple jurisdictions.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The fact that Hong Kong data law has been around for so long (since 1995!) and remains relatively unchanged today is a very interesting contrast to the pace of change in data regulation in other parts of the world – this is particularly the case because so many multinational companies have their Asia headquarters in Hong Kong, so the interplay in practice between different laws can become very complex and interesting as data itself often lives in more than one location in today's cloud-reliant business environment.

How is the privacy landscape changing in your jurisdiction?

Hong Kong's data and privacy laws definitely win the prize for longevity! They are due for a change (although I'm constantly amazed at the resilience of the PDPO and how well a law drafted in 1995 still holds up and adapts so well to so many novel practical situations in 2021). And as of 2020, we are finally seeing the beginnings of an earnest review of important areas for reform.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

In Hong Kong, phishing still remains one of the top tactics for bad actors to infiltrate systems. Threat actors are becoming more sophisticated and more patient and will wait longer to execute large-scale attacks, such as targeted emails to senior executives to trick them into transferring large sums of company.