PaRR
An Acuris company

PaRR Special Report

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC)

Preface

Dear Reader,

Big Data is emerging as the core business asset of the global economy. With China's new Cybersecurity Law a reality as of June this year and the EU's General Data Protection Regulation (GDPR) set to come into force in May 2018, actionable insight into these regulatory risks is now more important than ever.

Amidst this evolving environment, data protection regulators and executives from across the globe gathered in Hong Kong for the 39th International Data Privacy Commissioners Conference to map out the future of data protection and privacy in an increasingly connected world.

PaRR was on hand as public and private sector heavyweights discussed mechanisms to protect personal privacy while preserving the promise of seamless cross-border data flows. Assessing the risks, rewards and opportunities of this fluid data-driven landscape, *PaRR*'s event coverage lets you in on the thinking of data privacy authorities as they shape policies with the potential to inspire or inhibit the next wave of technological innovation.

Raymond Barrett
Managing Editor

Contents

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC)

03 Oct 2017

Localization, cross border transfers remain core issues for privacy commissioners, corporates

- Thirty-four countries have data localization laws; China and Russia take top slots
- Localization laws have become 'disjointed,' senior Apple Inc exec says
- EU-US Privacy Shield could be model for other jurisdictions, says former FTC chief

Data localization is the most contentious issue for privacy regulators and the increasingly data-driven global business community, data privacy professionals said in Hong Kong.

Localization, also known as data nationalism or data sovereignty, is the legal requirement to store data in the same country in which the data originates. Data localization laws are enacted to allow a "country to force a company to store data within their borders for regulatory, political and other reasons," according to Nigel Cory, a trade policy analyst.

Cory was speaking on a localization panel during day two of the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong on 29 September.

He said localization is a growing trend in which countries "across the political spectrum and at every level of development" are enacting barriers to data flows. It applies to all types of data, from accounting and tax data, to data related to health, individual services and telecommunications.

Cory estimated that 34 countries have data localization policies, with China and Russia having the most extensive localization regimes in place. Indonesia and Vietnam both intend to implement data localization policies, and Columbia and Brazil are likely to follow suit, he said.

Localization runs counter to the free flow of data –a core characteristic of the Internet – and constrains innovation, Cory said.

Go with the data flow

Panelist Jane Horvath, senior director of global privacy law and policy at Apple, said that while data localization started thirty years ago to ensure personal information was protected no matter where it flowed, localization laws "have become somewhat disjointed from the original aim."

The core question, said Horvath, is whether "the law should determine where data is stored" or should engineers make that decision "with the aim of delivering the fastest and most secure service."

"Where Europe has led on international data transfer obligations, others have followed," Horvath told conference attendees, adding that Apple was certified to APEC's Cross Border Privacy Rules system (CBPR) three years ago. The US tech giant's annual re-certification review to remain CBPR-compliant is more than a "check the box" exercise, Horvath said.

Horvath acknowledged some room for improvement in the CBPR system, but described CBPR as a "baseline for what compliance for international data transfer across multiple jurisdictions should look like", and said that could be built upon.

Horvath said localization creates redundant data sets that increase the exposure to threats, and give rise to the distraction

of diverse compliance requirements in multiple jurisdictions.

The Apple executive said that a "scratch below the surface" of legislative solutions revealed "laws designed to ensure access to data for surveillance purposes."

Courting change

Julie Brill, a former FTC commissioner currently serving as deputy general counsel for Microsoft, said cross border transfer accords, like the EU-US Privacy Shield, "could be a model for other jurisdictions".

"For instance, the Privacy Shield may serve as a reference point for Japan in its discussions with the European Commission about EU-Japanese data flows, and for China, as it evaluates potential mechanisms for satisfying its new cross border transfer restrictions," said Brill, alluding to China's new Cybersecurity Law.

Brill used China's Belt and Road Initiative (BRI) as a metaphor for international cooperation and information sharing, quoting Chinese President Xi Jinping's description of the ancient Silk Road on which the BRI is based. The Silk Road was a major artery of interaction, capital, technology, she said, an artery on which people flowed freely, and goods, resources and benefits were widely shared.

Brill said that today the Internet is the "vital artery of international interaction" and ensuring that data continues to "course freely through this artery is essential to our efforts to nurture progress, expand opportunity and promote prosperity."

One of the main concerns about – and justifications for – localization is law enforcement overreach; the US National Security Agency's mass data collection program exposed by Edward Snowden is often cited, although former Canadian Privacy Commissioner Jennifer Stoddart, also on the panel, suggested the US was perhaps not alone among nation-states in this respect.

Microsoft "strongly supports" passage of the proposed International Communications Privacy Act bill currently before the US congress to provide a "clear and fair" legal process to protect rights when the government seeks to access email and digital information.

Microsoft is challenging the US government's use of "indefinite and overly broad" secrecy orders that sought to prevent the company from telling customers when the government accesses their data. The suit, known as the 'transparency' case, goes to trial next June.

She noted that Microsoft has gone to court on several occasions to protect the personal privacy of consumers and customers "wherever they may be located."

Brill cited the landmark Warrants case, in which Microsoft sued the US government in 2014 "to prevent a warrant from compelling the company to produce email that was stored in a Microsoft data center in Dublin." Microsoft argued that a decades-old US law upholding the extraterritoriality of warrants did not outweigh the fundamental human right to privacy enshrined in the EU and Irish legal systems, as well as the rights of those who own the emails.

In July last year the US Court of Appeals for the Second Circuit ruled in the company's favor when it found that US warrants cannot be unilaterally applied to emails stored in other countries. In July of this year, the Department of Justice (DoJ) asked the US Supreme Court to take up the matter.

"In the context of localization, control can relate to national security concerns, which is part of the complex debate around data issues, especially regarding public data," trade policy analyst Nigel Cory, a panelist, told the gathering. "It's in the purview of each individual country to determine what they mean by national security, but the risk is that countries define national security so broadly, beyond what would be considered core issues, to many areas that are essentially commercial."

Cory, the trade policy analyst, suggested several motivations for nations to institute data localization policy, including the "mistaken rationale that localization will mitigate cybersecurity concerns," for purely mercantile ends, and to "facilitate government access to data."

by **Dave Lore** in Hong Kong

29 Sep 2017

'Notice and Consent' play core role in data protection, privacy architecture

- Hong Kong data privacy law incorporated the notion of consent
- Individual autonomy and control over data has to be valued

Data subjects should be given realistic and informed choices as a fundamental principle in data protection regimes, speakers at a Hong Kong data protection and privacy event agreed.

Stephen Wong, privacy commissioner at the office of the Privacy Commissioner for Personal Data (PCPD), said "notice and consent" is incorporated under the current Hong Kong law, which is in line with the requirements of the European Union (EU) General Data Protection Regulation (GDPR) that comes into force on 25 May 2018.

"There is no pressing need to change the law in this regard," Wong said in a speech at the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) on 28 September. However, the regulator will revisit other areas of the law, as reported.

The notice and consent process is a cornerstone of the foundation of trust and a core part of the architecture of the data protection and privacy commissioners' world, Wong said.

"One of our common values is without a doubt the interoperability and interconnectivity to ensure that personal data privacy is not only duly protected by also duly respected," Wong noted.

Meanwhile, Hong Xue, Director of the Institute for Internet Policy and Law at Beijing Normal University in China told a panel discussion that ubiquitous collection and processing of personal data cannot merit genuine consent.

Xue said data privacy protection should theoretically and practically value the individual's autonomy and control over his or her personal data.

"People are so accustomed to [consent forms] that most of them would not bother to read the lengthy privacy policy statement," Xue noted. Rather, it has become a tool for companies to obtain personal data legally, she added.

The EU's GDPR cost businesses heavily in seeking consumers' consent for collecting big data, since the law requires specification of use for the data subject, Xue said.

Companies must seek fresh consent from customers should they need to use the data for other purposes, Xue commented.

Naoko Mizukoshi, a Japan-based lawyer at Endeavour Law Office, said while medical data is strictly handled in Japan, there is a blurred definition as to whether data be treated as patients' health records or simply generic personal information akin to a postal address and mobile number.

There is much work to be done for the Japanese data regulator to explain to the public how collection of data could be used and its underlying risks, Mizukoshi said.

by **Candy Chan** in Hong Kong

29 Sep 2017

Cybersecurity focus diminishes data protection, UK official says

- Expanded focus on cybersecurity poses challenges for privacy
- Cybersecurity diverts resources from personal data protection

The UK data regulator will re-examine its policies as an "over-investment [and] over-emphasis" on cybersecurity could be a distraction from core focus of data protection, the country's top data regulator said today (29 September).

"I am worried many smaller agencies... think security is privacy," said Elizabeth Denham, head of the UK's Information Commissioner's Office (ICO), adding that a citizen's right to personal privacy is "fundamental" and it should not be given away to in lieu of cybersecurity.

Denham was speaking as a panelist at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) organised by the office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong.

The world is swamped with cybersecurity issues that will potentially diminish data privacy principles, which are equally important, Denham said.

Around 85% of civil voluntary penalties collected by her commission were related to data breach incidents, Denham said.

While data protection laws require organisations to protect data security, there is a lot more work needed in other areas and the commission will re-examine its regulatory policies, Denham added.

While taking a wait-and-see approach, Denham said she hopes the implementation of the EU's General Data Protection Regulation (GDPR) in May next year would help to improve the protection of personal data.

Frank Law, a senior superintendent with the Hong Kong Police Force's Cyber Security and Technology Crime Bureau (CSTCB) said there is a need to enhance cross-jurisdiction collaboration to track down data criminals.

It has been painful for law enforcers to collect evidence from overseas in data cases, especially since they are in a race with criminals, he added.

Timothy Pilgrim, acting head of the Office of the Australian Information Commissioner (OAIC), cited the willingness of the Australian Bureau of Statistics (ABS) to shut down its website after being hacked during last year's census as an example where data protection is not compromised in the name of cybersecurity.

by **Candy Chan** in Hong Kong

29 Sep 2017

Singapore data regulator embraces 'sandbox' to support digital economy

Singapore will deploy regulatory "sandboxes" to assist innovation in the digital economy, a senior official with the city-state's Personal Data Protection Commission (PDPC) said.

Speaking on a panel titled Data Protection in the East as part of the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Hong Kong on 28 September, PDPC Deputy Commissioner Yeong Zee Kin said Singapore wants to create a trusted eco-system that supports and rewards data innovation.

"The commission is prepared to work with companies…to create regulatory sandboxes so they are not held back from deploying technological and business innovations," he said.

This will help the PDPC as it works on fine-tuning Singapore's Personal Data Protection Act (PDPA) before it is amended, said Yeong.

A regulatory sandbox, often deployed in an innovative sector such as Fintech, is a 'safe space' where companies can test new products while not following all the existing legal requirements without the threat of enforcement or penalties.

When it comes to Singapore's data protection regime, the city-state is pivoting from compliance to accountability, Yeong said.

This necessitates a fundamental shift in corporate culture where consumer and corporate dialogue is key.

Singapore's data protection environment is somewhat different to other Asian nations, and Yeong pointed out that the country's data protection laws are enforceable by private civil action in the courts.

In July, PDPC announced a number of initiatives and Yeong told the conference attendees that Singapore's Data Protection Trustmark certification framework should be completed by the end of 2018.

An important goal of Singapore's data protection regime is to establish a high level of consumer trust and the PDPC is promoting a "data protection by design" approach.

In addition, the PDCD will not allow companies to hide behind badly drawn consent clauses, Yeong said, citing a recent case brought by the regulator.

by **Raymond Barrett** in Hong Kong

28 Sep 2017

US FTC worked with overseas agencies on major data breach case, says acting chief

- Companies can outsource data, but not their responsibility, Maureen Ohlhausen said
- Agency focuses on behavioural remedies, but can impose fines when statutes apply
- FTC pursues data privacy cases resulting in substantial injury to consumers

The US Federal Trade Commission (FTC) works with overseas enforcers and cooperated with Australian and Canadian regulators on one of the agency's largest data breach cases to date, the agency's acting chairwoman said in Hong Kong today (28 September).

Maureen Ohlhausen was referring to the AshleyMadison.com case, which according

to the FTC's official website involved the failure to protect the personal information of some 36 million registered users in 46 countries. She made the remarks at the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Each nation will develop its own institutions and approaches to personal data privacy, but the US has an extremely effective longstanding enforcement regime distinct from Europe's, Ohlhausen told PaRR, speaking to PaRR immediately following her participation on a panel comparing Asian with Western regulatory approaches to data privacy.

Ohlhausen said of the Privacy Shield – an EU-US framework governing personal data transfers to the US from the EU – that it is a "good system that we've negotiated and that we're trying to make sure it's up and running in a very robust way."

She declined comment on reports that European privacy regulators received complaints about the agreement and have themselves registered doubts about whether the accord meets EU privacy standards.

Ohlhausen also declined PaRR's request for clarification of recent US calls for China to revamp its new Cybersecurity Law.

On the panel, the acting FTC chief noted the critical importance of interoperability, and cautioned companies about the agency enforcement view of data outsourcing. Companies can "outsource their data, but they can't outsource their responsibilities," Ohlhausen said, adding that the agency has brought actions against companies "that made promises to consumers in the US but outsourced the data and didn't comply with their promises in the way that data was handled."

"Interoperability regimes are important," she stressed. "Companies will be held to their promises" regardless of where the data goes, she added.

Ohlhausen told attendees the FTC has brought "many, many" data security-related cases, "numbering some 500 cases" over time, and while she declined to disclose the number of active data cases, she did mention the FTC's ongoing investigation into the breach into US-listed Equifax, the Atlanta, Georgia-based multinational credit reporting agency.

She listed enforcement tools and remedies the agency has available under the FTC Act, which gives it the authority to go after companies that have deceived consumers or caused substantial injury.

"Much of our data breach enforcement has been under the second aspect of the law; breaches causing substantial injury to consumers" she said on the panel, adding that the agency has brought a number of cases against companies for having "inadequate data security protections".

The FTC has focused on "behavioural remedies", said Ohlhausen, such as compelling companies to undergo "ongoing monitoring, privacy audits, to provide information to consumers and report back to the FTC on its progress in protecting consumers" data.

In addition to the conduct remedies, she noted the agency has other sanctions at its disposal, citing the institution's recent data security case against Lenovo for a so-called man-in-the-middle attack, whereby the China computer giant allegedly preinstalled software on some of its laptops.

In a statement dated 5 September, the FTC said Lenovo agreed to settle charges brought by the FTC and 32 State Attorneys

Generals for harming consumers by "pre-loading software that compromised security protections in order to deliver ads to consumers".

Ohlhausen said that in addition to the conduct remedies, under certain statutes like the Children's Online Privacy Protection Act and Fair Credit Reporting Act, the agency has also been able to impose and recover fines "upwards of USD 7m".

by **Dave Lore** in Hong Kong

28 Sep 2017

Hong Kong data regulator to revisit local law in light of GDPR implementation

- Study revealed 20 differences between Hong Kong, EU privacy regimes
- EU set good example of sanctions, accountability principle
- GDPR could catch organisations outside EU

Hong Kong's data privacy law requires "revisiting" and "further exploration" in light of recent European rules and the borderless nature of personal data protection, according to the chairman at the office of the Privacy Commissioner for Personal Data (PCPD).

In the light of the implementation of European Union General Data Protection Regulation (GDPR) in May next year, the commission conducted a comparative study between Hong Kong and EU's regulations, in which 20 major differences were identified, Stephen Wong told PaRR.

The study was conducted with a view to recommending amendments to the Personal Data (Privacy) Ordinance to enhance the personal data privacy protection in Hong Kong, a PCPD spokesperson told this news service.

Wong was speaking at the 39th International Conference of Data Protection and Privacy Commissioners ("IPDPPC") today (28 September).

"GDPR is something Hong Kong businesses should pay attention to," Wong said, given the GDPR has explicitly strengthened its scope to non-EU organisations so long as the processing activities are targeting EU data subjects, he added.

The study revealed key issues would have to be reviewed because of the differences between privacy provisions in the two laws, Wong said, one of which relates to sanctions.

The EU set a "good example for the legal framework of penalising breaches," Wong said. The GDPR will levy administrative fines on companies of up to EUR 20m or 4% of the total worldwide annual turnover for the preceding financial year, whichever is higher.

Another issue is the "accountability principle" - which essentially refers to the various obligations organisations will have to follow in order to demonstrate compliance with EU data protection rules - is not covered in the Hong Kong ordinance, Wong said.

The PCPD will "further explore" the possibility of incorporating the accountability principle and certification regime in the city's privacy legal regime.

One means of the certification the PCPD is "seriously considering" is APEC's Cross Border Privacy Rules system (CBPR), Wong said at the event.

The CBPR is an APEC privacy code of conduct to regulate cross-border personal data transfers. It has 21 member countries, as reported.

"The key challenge is how to apply the core principles in data privacy protection which value individual's autonomy and control over his personal data," Wong said.

In order to help enterprises to understand the GDPR rules and their implications for businesses – including transfer of data outside and into Hong Kong – Wong said his office will publish a guidance in a few months' time.

Paolo Sbuttoni, a Hong Kong-based lawyer with Baker McKenzie, said during an earlier workshop organised by the law firm, that people in Asia do not realise that the GDPR can catch companies in Asia through extraterritorial effect.

Sbuttoni said the study carried out by the PCPD would be interesting because there is an absence of a clear law in Asia to address a number of key issues that arise with technology innovations and Artificial intelligence (AI).

There many gaps in the law which lags behind technology, Sbuttoni said.

by **Candy Chan** in Hong Kong

27 Sep 2017

Asian data officials advocate expansion of privacy rule system

Japan hopes to see expand and South Korea wants to fully participate in the Cross Border Privacy Rules system (CBPR), an APEC privacy code of conduct to regulate cross-border personal data transfers, officials from both countries told a forum in Hong Kong today (27 September).

Tsuzuri Sakamaki, Counsellor at Japan's Personal information Protection Commission (PPC), explained at the side event ahead of the International Conference of Data Protection and Privacy Commissioners ("ICDPPC") that Japan has been a member of the CBPR system since April 2014.

The APEC-endorsed system ensures privacy protections for cross-border transfers of personal information, Aakamaki told a CBPR workshop organised by the PPC, Japan's personal information protection commission.

There are only two certified CBPR accountability agents (AA) so far – one in the US, and one in Japan. The AAs perform tasks such as monitoring certified companies, dealing with relevant complaints and also enforcement.

JIPDEC – a non-governmental organisation which promotes the safe use of digital information – was recognised as Japan's first accountability agent in January 2016. Japan is currently the only Asian economy fully participating in the system, which currently comprises 21 member countries.

South Korea, Mexico and the US are members, while Philippines and Taiwan are taking steps to participate. Singapore is awaiting the results of its application to join, PaRR reported.

Masataka Saito, JIPDEC's director of accredited personal information, was enthusiastic about the certification of more AAs.

Jeong Soo Lee, deputy director of the privacy protection team cooperation team at Korea's Communication Commission (KCC), said the country already has identified some viable candidates to act

as Korean AAs. The Korean International Security Agency (KISA) is working to satisfy the system requirements, Lee told this news service.

She said liberal Korean lawmakers were advocating for a strong personal data protection system. They are very fervent about protecting Korean consumer rights, especially with regard to how such personal data is used or transferred out of the country.

by **Candy Chan** and **David Lore** in Hong Kong

27 Sep 2017

Singapore harmonizing cross border, domestic privacy regimes

Singapore is seeking to integrate its domestic data privacy regime with APEC's Cross Border Privacy Rules system (CBPR), according to a senior official with the city-state's Personal Data Protection Commission (PDPC).

Speaking on a panel as part of the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Hong Kong on 27 September, PDPC Deputy Commissioner Yeong Zee Kin said Singapore is currently waiting for the results of its application to join the CBPR system.

Of the 21-members of Asia-Pacific Economic Cooperation (APEC) Pacific-rim economic forum, the US, Japan, South Korea, Mexico and Canada have currently signed on to the CBPR—a voluntary privacy code of conduct for cross-border data flows.

Singapore has mapped its Trust Mark Certification Scheme—a generic standard which implements the country's Personal Data Protection Act (PDPA)—to certify compliance with CBPR, said Yeong.

"Our preference [is] to integrate the CBPR registration and certification as part of our domestic trust mark application," he said.

CBPR is an essential component in building a network of trust, said Yeong, who added that the process of integrating cross border and domestic data privacy is still a work in progress.

"We are still designing this system," he said. "We haven't made up our minds just yet."

Various branches of government were involved in this process and there was close consultation with companies in Singapore, said Yeong, adding that some of the ideas they shared with industry representatives were "sharpened" during that dialogue.

Yeong said Singapore was satisfied that the country's domestic laws meet the requirements of the GBPR.

Issues discussed by the panel included the challenges facing countries looking to join the system, such as the certification of domestic "accountability agents".

The CBPR's official website defines accountability agents as organizations that certify "the privacy policies and practices of participating companies are compliant with the CBPR system program requirements."

As Singapore is a very small economy compared to South Korea, Japan and US, Yeong said it is still uncertain how many accountability agents the Lion City can sustain.

by **Raymond Barrett** in Hong Kong

PaRR
An Acuris company

Asia
+65 6349 8064
parr-global.com