Asia, Africa Join the International Privacy Conversation

Europe’s privacy values still drive the conversation, but voices are emerging from the Philippines, Singapore, South Korea, Japan and elsewhere.
Foreword

In today’s increasingly connected world – marked by the proliferation of devices and services that communicate via the Internet and the emergence of Big Data – digital risks abound. Hacks and other data breaches are impacting an ever greater number of companies, governments and individuals. The potential costs in terms of business reputation, loss of privacy, regulatory fines and litigation are mounting. The spread of the so-called Internet of Things is only adding to the potential risks.

On September 25-29, 2017, officials from around the world gathered in Hong Kong for the 39th International Conference of Data Protection & Privacy Commissioners (ICDPPC). Membership in the ICDPPC includes more than 100 data-protection authorities in around 70 nations, including large countries and governmental units such as the US, the European Commission and the UK and smaller jurisdictions such as Andorra, Benin and Jersey.

While the range of topics discussed in Hong Kong was both broad and detailed, one issue pervaded the event: the upcoming implementation in May 2018 of the EU’s General Data Protection Regulation (GDPR). The heightened attention to data protection and privacy that is called for by the GDPR is something that regulators and businesses around the world are scrambling to respond to, leading to a truly global debate, because failure to adhere to the GDPR could cost businesses everywhere millions in fines. Perhaps equally important, the debate is underscoring the growing importance of data security and privacy to all.

MLex devoted a team of five reporters to cover this weeklong gathering, led by our Chief Global Digital Risk Correspondent, Mike Swift. In this special report, we highlight a selection of our coverage that focuses on many of the current and emerging themes in the area of data protection and privacy. While the issues involving digital risks are numerous, what is encouraging is that the number of voices joining the debate is increasing. MLex, as always, remains committed to providing our readers unrivaled coverage of that debate.
African nations discuss data protection cooperation, mull setting up permanent secretariat  

Head of global data-protection regulators’ group calls for oversight principles for intelligence agencies  

Regulations could help win trust for robots, but current frameworks remain scattershot  

Privacy regulators discuss data protection in connected cars, but thorny issues remain in regional data rules  

EU’s data security approach questioned amid emergence of alternative schemes  

Hong Kong will follow distinct privacy path from mainland China, privacy chief says  

Nuts and bolts of the EU’s General Data Protection Regulation

**Mike Swift**  
*Chief Global Digital Risk Correspondent*  
Formerly chief Internet reporter for the San Jose Mercury News and SiliconValley.com, Mike has covered Google, Facebook and Yahoo closely as he followed trends in search, the mobile web and online social networks. He helps coordinate MLex coverage of privacy and data security worldwide. A former John S. Knight Fellow at Stanford University, Swift is a graduate of Colby College. He is an award-winning journalist with expertise ranging from the business of professional sports to computer-assisted reporting.

**Tsering Namgyal**  
*Regional Correspondent, Hong Kong*  
Based in Hong Kong, Tsering Namgyal is a Regional Correspondent for MLex in Asia, specializing in financial regulations. He previously worked as an editor for Debtwire, also based in Hong Kong. He has also contributed to the Far Eastern Economic Review, the Asia Times, the Asian Wall Street Journal, the Financial Times, BusinessWeek and the South China Morning Post.

**Toko Sekiguchi**  
*Senior Correspondent, Tokyo*  
Toko is a senior correspondent in Tokyo covering antitrust, anti-bribery & corruption and regulatory issues. Before joining MLex, she worked as a journalist for Dow Jones News, Bloomberg News and Time Magazine.
African nations discuss data protection cooperation, mull setting up permanent secretariat

By Tsering Namgyal  |  September 25 2017

African nations are seeking ways in which they can enhance data protection across the continent through such possible initiatives as creating a permanent secretariat, it is understood.

Many African countries have taken a big leap forward in data protection by passing laws, but a number of solid steps still remain to be taken in such areas as beefing up skills, raising public awareness, and strengthening collaboration so that laws are enforced properly.

A proposal for a permanent secretariat for the Regional Dialogue on African Data Protection Agencies, or RAPDP, the umbrella body for the continent, was one such idea raised during a meeting of African data protection chiefs held on the sidelines of a global summit on the same topic in Hong Kong today.

The meeting was attended by data protection chiefs from such countries as Benin, Burkina Faso, Ghana, Mali, Morocco, Senegal and Tunisia, who discussed how best to work together.

They also said that in the future, leaders of a permanent secretariat could be democratically elected, rather than nominated as data protection chiefs currently are. The body’s key positions could be filled by representatives from different language zones as a nod to the continent’s linguistic diversity, said Awa Ndiaye, president of the Senegalese Data Protection Commission.

Patricia Poku, head of the Ghanaian Data Protection Commission, said the lack of...
a common language was a challenge, with the continent split between Anglophone, Francophone and Lusophone regions, among many other languages.

She also said that because things were “much slower in Africa,” having a dedicated secretariat would help in to make progress long term on data protection.

She said data protection, like climate change, was a cross-jurisdictional challenge and called for a collaborative approach.

Lahoussine Aniss, secretary general of the Moroccan Data Protection Agency, who is currently the head of the pan-African body, said that Africa nations needed to get their act together so they would not be criticized for being unable to reach a consensus.

Aniss said more discussion was needed on how such a body could be financed, and through what mechanism, but there was agreement that funding should come from within the continent.

Many African countries had already passed data protection laws, mostly modeled after the EU framework, and many were in process of enforcing those laws, said Ghana's Poku. They were roughly in line with Asian jurisdictions in terms of progress, but many development challenges needed to be addressed, she told MLex.

More discussion on how to strengthen collaboration will take place when Benin and Morocco co-organize the next RAPDP meeting, due to be held in Casablanca in December, members agreed.
Head of global data-protection regulators’ group calls for oversight principles for intelligence agencies

By Mike Swift  |  September 27 2017

The chairman of a global association of data protection and privacy regulators said the time has come for governments to negotiate a cybersecurity treaty that would establish principles for the conduct of intelligence agencies using electronic tools.

“We need to have an international treaty on cybersecurity, and on the actions of state actors,” John Edwards, chairman of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), said at the group’s annual meeting in Hong Kong this week.

Referring to the recent string of data breaches at companies such as Yahoo and the US consumer credit rating agency Equifax, “even large organizations can’t stay ahead of the malicious actors online, particularly where there are state actors involved,” said Edwards, who is New Zealand’s Privacy Commissioner.

In an interview on the sidelines of the conference, Edwards told MLex that the seemingly endless string of major data breaches constitutes “a market failure” that data-protection authorities must cooperatively address.

“We expect to accept that there is a level of risk” in using online tools and platforms, Edwards said, “but we don’t even know what the level of risk is.”

A unit of the ICDPPC, the International Working Group on Data Protection in Telecommunications, completed a working paper in April arguing that the world’s national data-protection authorities should promote seven guiding principles, including the right of individuals to have data minimized, deleted or corrected by intelligence agencies.

“There is a clear trend in calls for the creation of a new set of international principles to strengthen oversight of intelligence agencies and their information...
(including telecommunications information) gathering practices,” the working group concluded.

The paper found that civilian data-protection authorities “have a unique and valuable contribution to make” in the oversight of intelligence agencies, “and that their expertise and experience would be a positive contribution to the development of new principles.”

The string of commercial cybersecurity crises such as the breach that exposed more than 1 billion accounts in many countries at Yahoo, or the “WannaCry” ransomware that disabled computer networks around the world in May, illustrate the common denominator between the activities of national intelligence agencies and the vulnerabilities of commercial and government computer networks.

The WannaCry attacks were executed using software hacking tools stolen from the US National Security Agency, or NSA. The Yahoo breach, the US Department of Justice said in a criminal indictment unsealed in March, was executed by a group of hackers that included at least two members of the Russian Federal Security Service, or FSB, the successor to the Soviet Union’s KGB.

The Yahoo hack was part of a conspiracy to obtain access to personal accounts held by journalists, US and Russian government officials and employees at financial services, cybersecurity and private equity firms, the DOJ indictment said.

And the 2014 breach of US health insurer Anthem, the largest US data breach on record prior to the revelation of the Yahoo breach in 2016, was executed by state-sponsored actors operating from China, according to court filings in US litigation brought over the case. Anthem recently agreed to pay $115 million to settle the allegations in US district court brought by the class action plaintiffs.

Reliable information has not yet become public about the attackers behind the Equifax breach, which exposed the Social Security numbers and other information on 143 million people – more than half of the US adult population.

Edwards said that since the revelations of the former NSA contractor Edward Snowden about electronic intelligence gathering in 2013, it is no longer viable for
intelligence agencies to simply disavow that they intercept email and conduct other surveillance of the Internet and other electronic communications. New Zealand is one of the so-called “Five Eyes,” the intelligence alliance that also includes Australia, Canada, the US and the UK.

The thrust of any effort by data-protection authorities to outline principles of conduct for electronic surveillance does not mean that they are trying to stop electronic intelligence-gathering, Edwards told MLex. “It’s a legitimate activity of a state. We have to recognize that,” he said.

Among the seven proposed principles for the oversight of international intelligence services identified by the ICDPPC working group was that they operate with a clear legal mandate and authorization framework, and that the collection of personal information should be limited to the least intrusive means of collection.

Cybersecurity and privacy oversight principles for electronic intelligence-gathering “does need to be a coordinated, international approach,” Edwards said.

Membership of the ICDPPC includes over 100 data-protection authorities in about 70 nations, with members ranging from large countries and governmental units such as the US, the European Commission and the UK to data protection authorities for smaller jurisdictions such as Andorra, Benin and Jersey.

Edwards was appointed New Zealand Privacy Commissioner in February 2014.
Regulations could help win trust for robots, but current frameworks remain scattershot

By Tsering Namgyal  |  September 28 2017

Regulatory frameworks are grossly ill-equipped to deal with robots even as the behavior of machines that mimic human intelligence seem to be becoming less predictable, according to experts.

At issue is the extent to which machines can be trusted and, if not, how to ensure that they are made more reliable and obedient to human masters who deploy them to perform tasks with various levels of sophistication.

Regulations could help establish “trust by proxy,” Urs Gasser, head of the Berkman Klein Center for Internet and Society at Harvard University, told a panel discussion held on the sidelines of a global data privacy conference in Hong Kong.

“You may not trust the technology, but there is a remedy or a protection” in the form of regulations, he said.

Yet, devising regulations for robots is made challenging by a number of factors, experts said, including the question of whether and how human ethical norms can be extended to machines, as well as the debate over who should be held accountable in the event of accidents or data breaches.

The key question is whether robots or those who design them are to be trusted.

One of the reasons why robots, which are based on algorithms, are seen as behaving erratically is because the “level of abstraction is too broad,” and scientists are often

Continued on next page
“optimizing the wrong things,” Suresh Venkatsubramaniam, a computer science guru at the University of Utah, said.

“This is partly the reason why the laws in the US are unable to capture AI [artificial intelligence],” he said.

Experts agree that it is often hard to explain how and why robots act in a certain way.

“AI does a random walk and does not explain how I got there,” Venkatsubramaniam said.

The challenge of “explainability” can be attributed to the fact that the techies who design these machines do not often communicate their ideas well with lawyers, ethicists and regulators involved in the field, and who often look at them through frameworks otherwise designed for humans.

Gasser of Harvard’s Berkman Center acknowledged that there is a “semantic interoperability” between different fields involved in AI and machine learning.

The term artificial intelligence is also becoming hackneyed, because it is “being overused and is no longer useful as a concept,” Venkatsubramaniam said.

Regulatory frameworks and guidelines governing the field, not surprisingly, remain sketchy at best, even as AI is being widely adopted in a wide range of industries.

AI is used by banks in Hong Kong to face customers, by cucumber farmers in Japan and by the healthcare industry in countries such as Singapore, not to mention technology multinationals such as Google in its famous self-driving cars.

China is seen an emerging global leader in AI, with Beijing having issued a lengthy guideline earlier in the summer promising to “fully propagate new achievements in AI.” Danit Gal, a China-based AI expert, said that the document was aimed at rallying public support for AI.

Yet, like all innovation in China, the issue of trust and privacy is taking a backseat, because the priority now is on gaining an early foothold and establishing China as a leader in AI.

The attitude of regulators at this stage is to leave the tricky issues of risk

Continued on next page
management – and the philosophical and legal debates about ethics – to be addressed later, once things have gained critical mass.

China is expected to become a global leader in AI by 2020 mainly because Chinese companies are sitting on enormous amounts of data and the government wants to persuade the public to give consent to the use of such data for the development of AI, Gal said.

Chinese technology titans such as Baidu, Tencent and Alibaba are pouring billions into the new technology, it is understood.

The Japanese government in July, meanwhile, announced guidelines on AI aimed at developing safety standards, which is likely to be presented at a meeting of the G7 in the fall, said Tatsuya Kurosaka, a professor at Keio University.

Tokyo’s current position is to frame the debate around AI regulations within the context of “human well-being,” and this yardstick is likely to be applied to all the regulatory approaches governing robots in the future, he said.

The question of how AI can be regulated is made challenging by the fact that AI is applied across different industries that come under different regulatory bodies.

One way forward could be industry-specific regulations, as was seen in Germany, which published ethical guidelines governing autonomous cars last month.

Unlike in the financial sector, where regulators are increasingly rolling out regulation-free zones known as “sandboxes,” no such testbeds have yet been rolled out for other sectors to gauge their risks to humans before they are introduced on a large scale.

This begs the question of whether there is a need for a so-called “Delaware for AI,” said Harvard’s Gasser, pointing to the example of the US state where regulatory exemptions are granted for new innovations.

More than 90 percent of the respondents to a survey conducted by the organizer of the panel, the think tank Digital Asia Hub, responded “not yet” when asked if they trusted AI, highlighting the trust deficit that must be bridged for AI to be gain wider public acceptance.

The question about whether robots can be relied upon came to light recently when robots developed by Facebook were shut down after they started talking to each other. The Chinese government also took down two robots after they reportedly said “no” when asked if they loved the Communist Party.
Privacy regulators discuss data protection in connected cars, but thorny issues remain in regional data rules

By Toko Sekiguchi and Mike Swift | September 28 2017

An international forum of the world’s privacy regulators said on Thursday that they had adopted resolutions on data protection for connected vehicles in an attempt to stay one step ahead of businesses bringing smart cars from the drawing board to the road.

This year’s International Conference of Data Protection and Privacy Commissioners also comes as industries and regulators around the world scramble to prepare for the implementation of the EU’s strict General Data Protection Regulation, or GDPR, next year. Sideline discussions underscored the fundamental differences between jurisdictions like the EU, which place a heavy burden on companies when it comes to data breaches, and those reluctant to introduce penalties for fear of businesses shying away from utilizing Big Data.

The conference’s resolution on connected vehicles, from which the US representative – the Federal Trade Commission – abstained, was aimed at manufacturers and transportation services as carmakers increasingly look to Internet-of-things technology for growth opportunities.

One key element of the resolution related to privacy protections for artificial intelligence algorithms that would be built into computer systems in connected cars. As approved, the resolution requires that the “self-learning algorithms needed for automated and connected cars are made transparent in their functionality and have been subject to prior assessment by an independent body in order to reduce the risk of discriminatory automated decisions.”

People familiar with the discussion said that the US, concerned about the impact on technological innovation, had objected to making the algorithms subject to pre-approval by an independent body, and refused to approve the resolution with that language included.

Giovanni Buttarelli, the European data protection supervisor, told MLex on the sidelines of the conference that he viewed the connected car resolution as one of the most significant accomplishments of this year’s conference. He said the conference

Continued on next page
needed to stake out a global position on privacy and data security for connected cars because they were moving from the design desk to the market, and regulators’ influence was at its peak now.

“It’s becoming a reality,” Buttarelli said. “That is the right moment to approach the issue, on a global scale. Not regionally.”

Privacy regulators from Asian jurisdictions also highlighted the specific needs and environments that gave rise to their countries’ data protection laws – often modeled on those in Europe but varying in enforcement due to different legal systems and economies in an age of e-commerce in which 121 countries had adopted some type of privacy laws.

Raymund Liboro, the privacy commissioner and chairman of the Philippines’ National Privacy Commission spoke of the importance of data protection in his country, where the outsourced customer service sector was a vital part of the economy.

“Handling personal data of multiple countries is an important economic strategy,” Liboro said, as he described one of the region’s newest, yet also most stringent, privacy rules governing business.

The group also adopted resolutions recognizing the need for increased collaboration between data privacy and consumer authorities, and exploring options for international enforcement cooperation.

But the balance between privacy and innovation remained an issue for regional agreements, alongside the severity of enforcement in different jurisdictions. A voluntary Apec-based data transfer scheme known as the Cross Border Privacy Rules has only five participating states: US, Mexico, Canada, Japan and South Korea – with fewer than two dozen companies certified from Japan and the US.

Although its officials hail the CBPR as an Apec counterpart to the European GDPR, what stands out is its low rate of participation and standards.

Tsuzuri Sakamaki, a counsellor for Japan’s Personal Information Protection Commission, told MLex that large data breach penalties were not suitable for countries like Japan, whose companies maintain “a high-quality compliance corporate culture.”
EU’s data security approach questioned amid emergence of alternative schemes

By Toko Sekiguchi  |  September 29 2017

Data professionals and privacy experts have identified what they say are problems with the European Union’s restrictive adequacy approach to ensuring secure cross-border data flows. They highlighted those issues at an international conference of privacy commissioners in Hong Kong as they pointed out that other regional rules used methods such as voluntary certifications to secure data transmissions.

Bruno Gencarelli, the head of the European Commission’s International Data Flows and Protection Unit, emphasized the need for adequacy measures in a global arena in which more than 120 countries had data privacy laws based on local legislation, enforcement and supervisory boards.

“Adequacy findings essentially assimilate a third-party country to a member of the EU, allowing a free flow of data,” Gencarelli said, adding that the EU was not looking for “carbon copies” of its own system, but seeking convergence with a nod to cultural diversity when it came to privacy protection.

Jennifer Stoddart, Canada’s former privacy commissioner, spoke highly of the EU’s recently expressed position on adequacy, which she said had “really been a milestone in terms of international data protection standards.”

However, while acknowledging that measuring an adequate level of protection may be the best means of managing international data flows, she said much work needed to be done to consider data exchanges in the context of national security systems, including those of EU states.

Shell International’s data privacy legal counsel, Monika Tomczak-Gorlikowska, also said that smaller suppliers and service providers to large multinationals that operated globally could suffer under the adequacy system, and that more transparency was required. “They need the ability to demonstrate that trusted partners can meet the same requirements,” she said.

Raymund Liboro, the privacy commissioner at the Philippines’ National Privacy Commission, spoke of the Apec Cross Border Privacy Rules system, or CBPR, a certification framework for the Asia Pacific region whose current members are the US, Mexico, Canada, Japan and South Korea, raising the question of how accountability could operate in a voluntary, cross-jurisdictional framework.

Gencarelli said the CBPR’s certification-based system differed from the EU’s rules in terms of safeguards, the exercise of individual rights, and enforcement. Although he said that EU was always looking for ways to bridge the gaps between different systems, it was “too early to talk about mutual recognition.”

Much work needs to be done to consider data exchanges in the context of national security systems.
Hong Kong will follow distinct privacy path from mainland China, privacy chief says

By Mike Swift  |  September 29 2017

Hong Kong’s data protection chief sought to draw a clear distinction today between the privacy and data security laws – and cultural values – of this Chinese special administrative region and mainland China, saying Hong Kong will always protect the privacy of international data flows of multinational companies.

Speaking on the sidelines of an international data protection conference, Stephen Kai-yi Wong, the privacy commissioner for personal data in Hong Kong, said that European Union-style laws that define privacy as a fundamental human right were passed before the handover of Hong Kong to China in 1997.

“Hong Kong regards this right as a fundamental human right,” Wong said in an interview with MLex. “Not necessarily in other emerging economies. One of the emerging economies is mainland China, our motherland. We have a difference – not only in terms of regulatory framework, but also in terms of privacy culture. That’s obvious.”

Under the “One Country, Two Systems” mechanism that was part of the handover of the former British colony to China, Hong Kong will maintain its own legal system for 50 years from the 1997 handover.

In hosting data protection and privacy regulators from more than 70 countries this week, Hong Kong has promoted itself as a global hub that helps multinationals, including banks and insurers, to deal with cross-border transfers of data amid tighter regulatory scrutiny around the world.

Given the close parallels between EU law and Hong Kong’s privacy legislation passed in 1995, when Hong Kong was still a colony of the UK, Wong said it is “a matter of formality” that Hong Kong will qualify for a data protection “adequacy” finding by the EU. Such a finding would allow Hong Kong to handle the international flow of data about Europeans, just as if Hong Kong were an EU member state.

“I believe that this is a matter of time,” Wong said. The EU is “talking about [South] Korea; they are talking to Japan. It’s not our turn yet. But we are prepared. We stand ready not only to meet the requirement, but in terms of operation and performance, we will reach the same standard” of EU privacy protection.

Wong’s office has made a point of using online social networks that are blocked in...
China, including Facebook and YouTube, to promote its privacy agenda. Hong Kong has more than 5 million Facebook accounts, he said, noting that this total comprises more than half of Hong Kong’s population.

“These are the changes we want to bring to the attention of our friends…in the West,” he said.

In his interview with MLex, Wong drew not just a legal, but also a cultural distinction between Hong Kong and the mainland. While both share Confucian values, he said, Hong Kong has come to value the rights of the individual in a way that is different from the mainland.

“In Hong Kong, we follow the EU model – that is, that a data privacy right is a fundamental human right, and we are talking about the fundamental rights of individuals. In mainland China, correct me if I am wrong, they are more on the side, in terms of a line of thinking, as the Americans. It’s more on the communities, the national interest, than on the individual’s rights.”

The mainland and Hong Kong even have a different way of writing “privacy,” Wong said, noting that Hong Kong and the mainland use the same two Chinese characters, but write them differently. “Perhaps, they would like to differentiate their notion of privacy from ours, so they reverse the order” of the two characters, he said.

“The Cultural Revolution [in mainland China] was just 50 years ago. They have a different political and historical background that would affect the notion of privacy: ‘What do you mean, this is your secret, your privacy? I’m your boss. I’m a leader of the [Communist] party,’ “ Wong said, playing the role of a party official.

Wong said he has “no doubt” that the legal distinctions between privacy in Hong Kong and mainland China will persist, in part because it is in the interests of mainland China. He referred to the experience of the Chinese e-commerce and cloud computing giant Alibaba, which has been expanding its services in Hong Kong and elsewhere in Southeast Asia.

Alibaba said in February that it had more than doubled the capacity of its Hong Kong data center “to address the increasing demand for secure and scalable computing services in Asia Pacific.”

“In terms of data transfer, I’m sure it must be a reason for [Chinese officials] to consider seriously. Alibaba, the amount of data they have collected, will they say, ‘who cares’” if China were to interfere in data flows? Wong said.

“No, they won’t. They mustn’t. So, in terms of this right, I’m sure that China will look at the ways we have been doing it seriously.”
Nuts and bolts of the EU’s General Data Protection Regulation

**TOUGH PENALTIES**

- Fines of up to 4% of annual global revenue or €20 million, whichever is greater

The regulation applies to non-EU companies that process personal data of individuals in the EU. The international transfer of data will continue to be governed under EU GDPR rules.

The definition of personal data is now broader and includes such identifiers as genetic, mental, cultural, economic, and social identity.

**Obtaining consent** for processing personal data must be clear and must seek an affirmative response.

Data subjects have the right to be forgotten and erased from records.

Parental consent is required for processing of personal data of children under age 16

Users may request a copy of personal data held by companies in a portable format.

Controllers must report a data breach no later than 72 hours after becoming aware of the breach, unless the breach has a low risk to the individual’s rights.

The appointment of a data protection officer (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk assessment will be required for projects where privacy risks are high.

Products, systems and processes must consider privacy-by-design concepts during development.

Data controllers must ensure adequate contracts are in place to govern data processors.

Data processors can be held directly liable for the security of personal data.

Controllers must have a legal basis for processing and collecting data.

One stop shop: international companies will only have to deal with one supervisory data protection authority.

YOU HAVE TO COMPLY WITH EU GDPR BY MAY 2018
MLex’s unique insight, analysis and commentary delivers investigative and forensic coverage of cases working their way through decision-making bodies and regulatory agencies around the world.

Regulatory change is coming. Be ready. Be the first to understand how regulatory change impacts your clients. Request a free trial.