MAYER·BROWN

International Developments in Privacy Law and Vendor Agreements

Lei Shen

Qi Chen

Oliver Yaros

Speakers

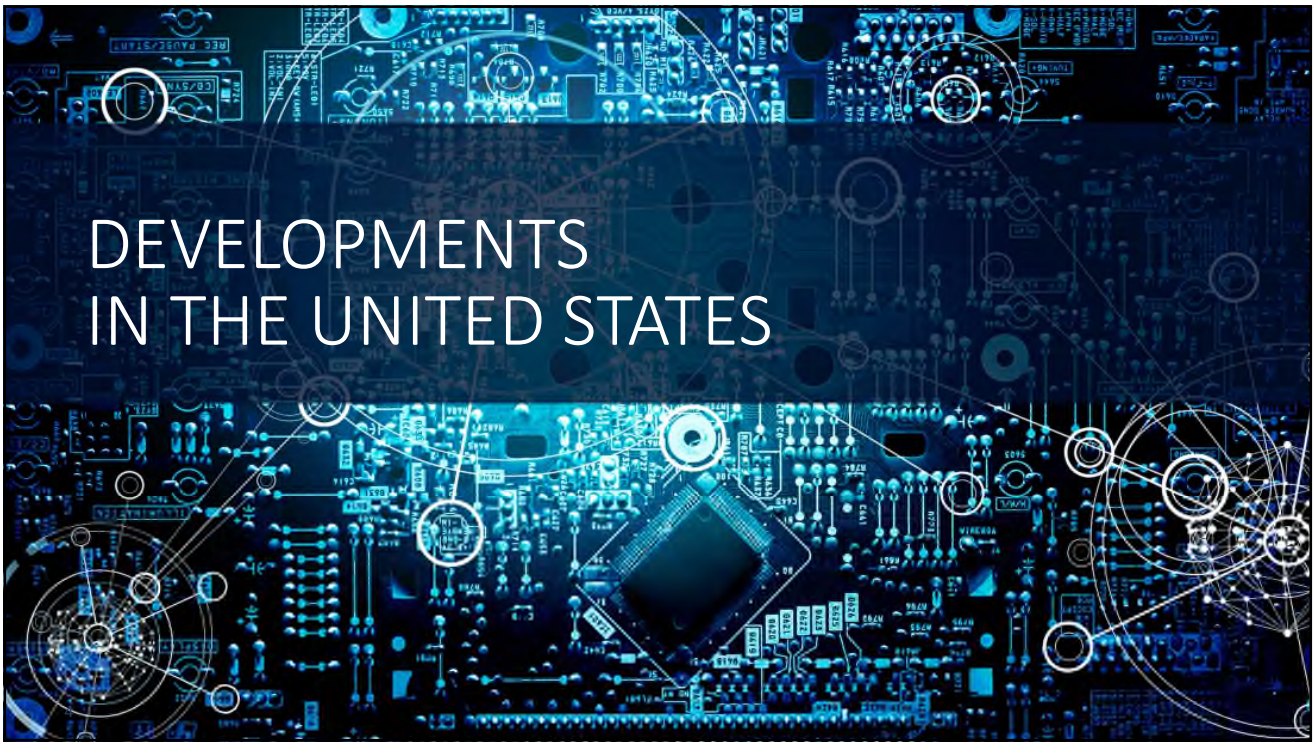
Lei Shen

Qi Chen

Oliver Yaros

Agenda

- Developments in the United States
- Developments in the APAC Region
- Developments in the European Union
- A Jurisdictional Comparison of Data Breach Notification Laws



New Data Breach Notification Laws

- All 50 states have data breach notification laws
- South Dakota and Alabama were the last states to enact these laws
  - South Dakota: enacted March 21, 2018, effective July 1, 2018
  - Alabama: enacted March 28, 2018, effective May 1, 2018
- Trends in data breach notification laws
  - Protection of health information and account information
- Trends in notification timeframes
- Impact on vendor agreements

New Trends in State Laws

Biometric Data

- State laws regulating use of biometric data
- Washington joins Illinois and Texas with this type of law
  - Regulates manner in which businesses can use biometric information
  - Requires notice and consent
- Supplements state data breach notification laws' coverage of biometric data
- Impact on vendor agreements

New Trends in State Laws

Cybersecurity Regulation

- Expansion of sector-specific cybersecurity regulation
- New York Department of Financial Services ("NYDFS") Cybersecurity Regulation for banks and insurers
  - Mandates cybersecurity standards for financial institutions
  - Impact on vendor agreements
- Other states are following this trend (e.g., Colorado and Vermont)

DEVELOPMENTS IN THE APAC REGION

China's Cybersecurity Law

- Effective as of June 1, 2017
- Covers government entities, operators of critical information infrastructure ("CII"), and network operators.
- Contains data localization requirements, cross-border transfer of personal information and important data requires a security assessment.
- The law is very high-level and vague, will be supplemented by regulations and standards yet to be officially published.

Draft Regulations and Guidelines

- Along with the Cybersecurity Law, the Cyberspace Administration of China ("CAC") released draft versions of legislation that would supplement the Cybersecurity Law.
  - Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data: will expand the data localization requirement to network operators.
  - Assessment Guidelines for Security Assessment of Cross-border Data Transfer: provides additional details on the security assessment process and clarifies the concepts for domestic operation and cross-border transfer.
  - Regulation for the Security Protection of the Critical Information Infrastructure: will further define the scope of Critical Information Infrastructure and the obligations on operators of CII

Personal Information Security Specification

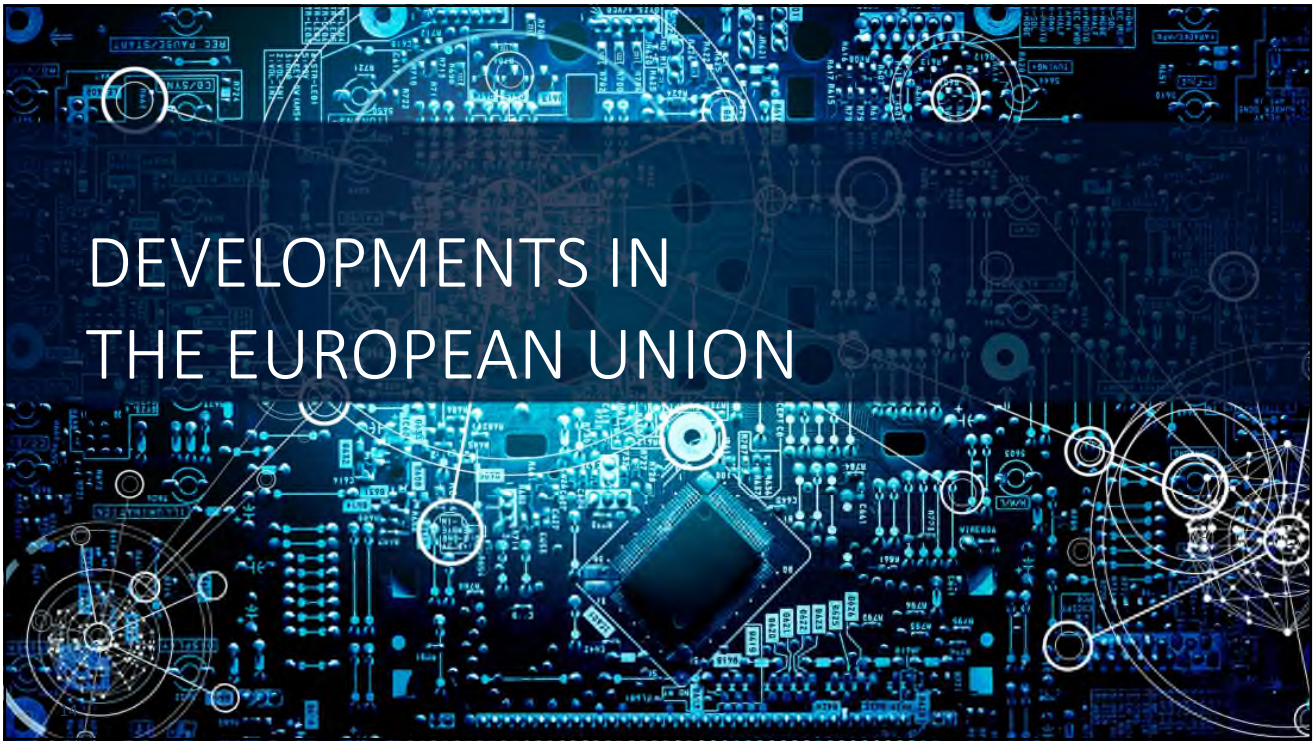
- Information Security Technology – Personal Information Security Specification released on December 29, 2017 by the National Information Security Standardization Technical Committee ("TC260") and came into effect on May 1, 2018.
- Voluntary and not legally binding, but will supplement regulators in the enforcement of cybersecurity laws and regulations such as the Cybersecurity Law.
- Largely aligned with the Organization for Economic Development ("OECD") privacy principles such as the principle to limit collection of personal information to what is required for carrying out the relevant business activity and to be transparent about the purpose of collection and use of personal information.

Australian Privacy Amendment

- Privacy Amendment (Notifiable Data Breaches) Act 2017, passed in February 2017, took effect in February 2018.
- Establishes a mandatory data breach notification scheme requiring all entities currently covered by the Privacy Act to provide breach notices to affected individuals and the Australia Information Commissioner (Commissioner)
- Only applies to "eligible data breaches" – breaches involving personal information that are likely to result in serious harm to any individual affected.

Rapid Pace of Change

- **SINGAPORE** – New Cybersecurity Bill passed in February, 2018. Will have licensing standards for cybersecurity service providers.
- **VIETNAM** – Latest Draft Bill proposed published November 23, 2017, will likely have data localization requirements.
- **THAILAND** – Draft Bill proposed May 24, 2017. Will give the government broad rights over private entities (injunctive power and information access rights) in the name of cybersecurity.
- As a whole, the APAC region is rapidly moving towards more regulations in this area, with a focus on 1) matching the EU GDPR regime or 2) protecting national interests.



Developments in the European Union

- The General Data Protection Regulation ("GDPR"): Effective 25 May 2018
- The Network and Information Systems ("NIS") Directive: The deadline for implementation into national law is 9 May 2018
- The ePrivacy Regulation: Not finalised but may be adopted later in 2018

The GDPR: The Key Changes

- **A Regulation, not a Directive**: The GDPR will be directly applicable in the same form in all EU Member States with the intention of reducing the burden on international organisations
- **Changes to territorial scope**: In addition to businesses that are established in the EU, non-EU businesses that process personal data in relation to the offer of goods or services to individuals within the EU, or as a result of monitoring individuals within the EU, will now have to comply
- **Significantly higher fines:** The maximum fine will be substantially increased to 4% of an enterprise's worldwide turnover or €20 million per infringement, whichever is higher
- **New data loss notification obligation:** The relevant European DPA must be notified without undue delay and where feasible within 72 hours. The individuals affected may also have to be notified
- **New data privacy governance requirements:** A data protection officer may have to be appointed to be responsible for an organisation's compliance. Organisations will also be required to map their processing activities and undertake data protection impact assessments for higher risk processing
- **A requirement to implement "privacy by design":** Businesses must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken
- **Strengthening of individuals' rights to personal data:** Individuals will have the "right to be forgotten," the "right to data portability" and the right not to be subjected to automated data profiling
- **Obligations on both data controllers and data processors:** Service providers will be held accountable for their own level of appropriate security, must document their processing to the same extent under the GDPR and must obtain prior consent to use sub-processors

The NIS Directive: The Requirements

- **A Directive, not a Regulation**: National law is required in each EU member state to implement the NIS Directive. The deadline for this to happen is 9 May 2018.
- **Applies to "operators of essential services" ("OES"):** Those entities that provide a service that is essential for the maintenance of critical societal and/or economic activities, the provision of which relies on network and information systems, and in respect of which a cyber incident would have a significant disruptive effect on the provision of the service. E.g., financial services, drinking water supply and distribution, energy, health, transport, etc. Member states must identify those entities they consider as being operators of essential services in their jurisdiction by November 2018.
- **Applies to "digital service providers" ("DSPs"):** Those entities that provide online marketplaces, online search engines and/or cloud computing services. Applies to digital service providers inside the EU and those offering services to the EU. DSPs that have a turnover below €10m or employ fewer than 50 people are exempt.
- **Adoption of a national strategy for cyber security:** Member states must introduce a national framework to manage and share information about cyber security incidents. This will involve the creation of a National Cyber Security Strategy, a Computer Security Incident Response Team ("CSIRT" – the National Cyber Security Centre ("NCSC") in the UK) and national NIS competent authorities.
- **Adoption of outcome based on high-level principles for security:** Both OES and DSPs will be required to take appropriate measures to prevent and minimise the impact of incidents affecting their network and information systems, with a view to ensuring the continuity of those services. Member states must introduce principles to be adhered to in order to secure the technology, data and networks used by OES. For DSPs, it is likely that separate principles will be produced, aligned with the guidance published by the European Network and Information Systems Agency ("ENISA").
- **New data loss notification obligation:** The competent authority must be notified of an incident having significant/substantial impact without undue delay (and within 72 hours where feasible in the UK).
- **High fines for noncompliance:** The maximum fine will be 2% of an enterprise's worldwide turnover or €10 million per infringement for lesser offences or 4% of an enterprise's worldwide turnover or €20 million per infringement for failure to implement security measures (but €20m only in the UK)

The ePrivacy Regulation: The Potential Changes

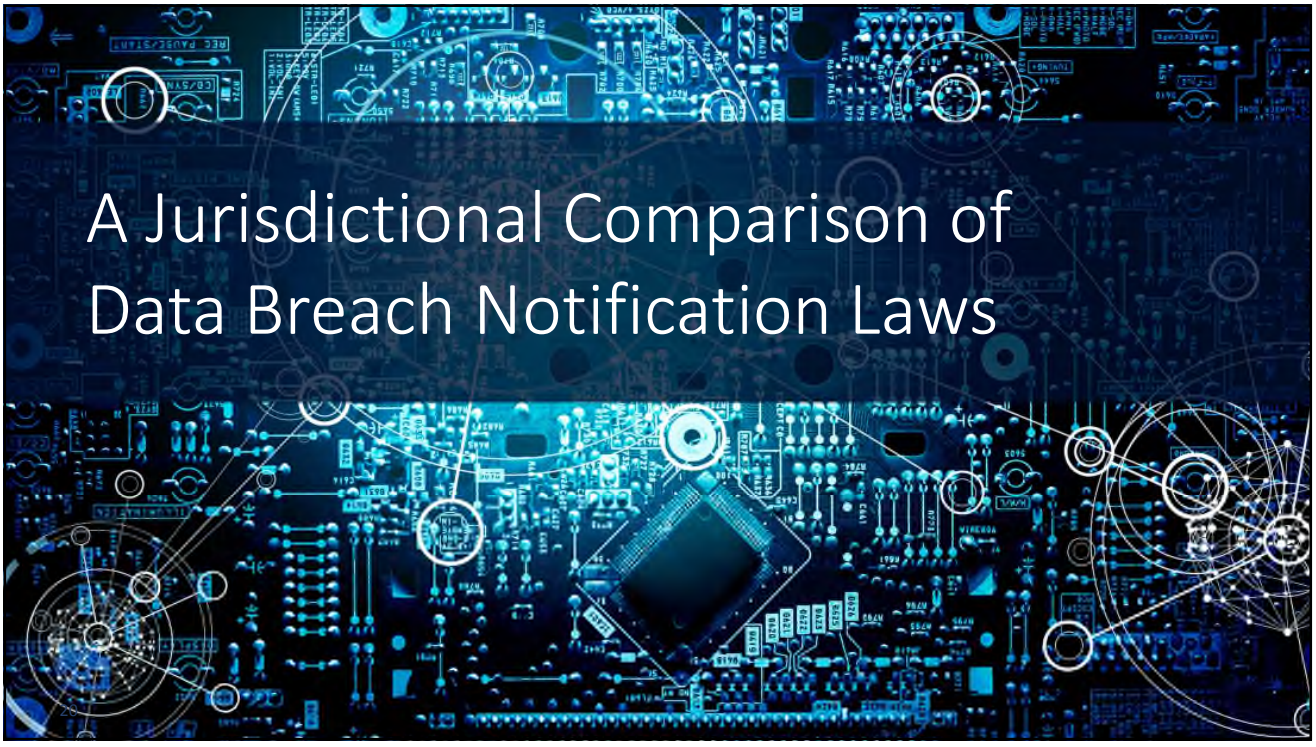
- **A Regulation, not a Directive**: The ePrivacy Regulation will replace the Privacy and Electronic Communications Directive. The Regulation is not yet finalised and it is unclear when it will be adopted – potentially later in 2018.
- **Applies to the storage of information in or related to a user's devices:** The use of cookies and similar technologies is prohibited unless consent is obtained, it is necessary for providing a service requested by an end user, it is necessary to transmit an electronic communication or it is necessary for web audience measuring by the provider providing the service requested by the user.
- **Applies to the sending of unsolicited electronic marketing communications**: Prohibits the transmission/instigation of the transmission of unsolicited direct marketing communications unless the recipient has previously notified the sender that he consents, for the time being, to being sent marketing communications by or at the instigation of the sender (an opt-in).
- **Changes to the current "soft opt-in" for marketing communications**: An opt-in is currently not required where:
  - The sender has obtained the recipient's contact details in the course of a sale or negotiation for the sale of a product or service to the recipient
  - The direct marketing is in response to that person's similar products and services only
  - The recipient has been and is given in every communication a simple means to unsubscribe.

  Under the draft ePrivacy Regulation,* business to business communications in addition to business to consumer communications may be covered and the right to rely on the "soft opt-in" for negotiations may be removed.
- **High fines for noncompliance:** The maximum fine will be 4% of an enterprise's worldwide turnover or €20 million per infringement for failure to implement security measures.

*October 2017

The Implications for Vendor Agreements

- **Service providers that use personal data in scope of the GDPR:** Ensure that the Article 28 requirements are addressed. Specifically:
  - The contract must include a description of the subject matter and the duration of processing, its nature and purpose, as well as the types of personal data being processed in respect of which categories of data subjects.
  - There must be an obligation on the vendor to assist with requests under Articles 32 to 36 of the GDPR, which include assisting with notifying a supervisory authority or a data subject of a data breach and conducting data protection impact assessments.
  - The vendor must agree to assist with respect to requests from data subjects that are exercising their rights under the GDPR.
  - The vendor must make available all information necessary to demonstrate compliance and must allow for and contribute to audits.
  - The vendor must ensure that all of its personnel who process personal data are bound by confidentiality obligations.
  - The contract must require the vendor to delete or return all of the personal data at the end of the services (unless required by EU law).
- **Agreements with DSPs: Consider whether your organisation or the service providers you use count as DSPs:** Consider whether the service providers you use need to contractually commit to taking appropriate measures to prevent and minimise the impact of incidents affecting their network and information systems, with a view to ensuring the continuity of those services in compliance with the high-level principles under the NIS Directive.
- **Agreements with website operators, advertising partners, lead generators, etc:** Consider whether the service providers you use to operate your website, generate leads and conduct marketing on your behalf will comply with the consent or other requirements for the cookies and other technologies they use and the marketing leads they provide you with/marketing campaigns they conduct under the ePrivacy Regulation.



Comparison of Data Breach Notification Laws

	SCOPE
United States	• Mostly limited to personal information that could put a person at risk for identity theft • Mostly limited to computerized data
EU GDPR	• Covers all personal data, subject to risk analysis • Covers all forms of personal data
Australia	• Covers all personal data, subject to risk analysis • Covers all forms of personal data
China	• Covers all personal data, subject to risk analysis • Covers all forms of personal data

Comparison of Data Breach Notification Laws

	DEFINITION OF BREACH
United States	• Typically requires "unauthorized access or acquisition" of covered information
EU GDPR	• Accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
Australia	• Unauthorized access or disclosure (or the likely unauthorized access or disclosure in the event of loss) of personal information that would likely result in serious harm to the related individual
China	• Events that cause harm to the network and information systems or data therein due to human factors, hardware and software defects or failures, or natural disasters, and which have a negative impact on society

Comparison of Data Breach Notification Laws

	NOTIFICATION TIMEFRAMES
United States	• Controller: fastest is 30 days • Processor: fastest is 24 hours
EU GDPR	• Controller: 72 hours to supervisory authority; without undue delay to individuals • Processor: without undue delay
Australia	• Carry out assessment within 30 days after becoming aware • As soon as practicable to the Privacy Commissioner • As soon as practicable thereafter to the affected individuals
China	• For breaches considered Significant or Very Significant, immediately report the incident to the appropriate governmental agency in accordance with the National Cybersecurity Incident Response Plan (NCIRP). • For other levels of breaches, timely report the incident to the appropriate governmental agency in accordance with the NCIRP. • Timely report to affected individuals

Comparison of Data Breach Notification Laws

	WHOM TO NOTIFY
United States	• Notify affected individuals • Notify a variety of state and other agencies (e.g., law enforcement, state attorneys general, credit reporting agencies, etc.)
EU GDPR	• Notify affected individuals • Notify supervisory authority
Australia	• Notify affected individuals • Notify the Privacy Commissioner
China	• Notify affected individuals • Notify the relevant government entity in accordance with the NCIRP

Comparison of Data Breach Notification Laws

	LIABILITY AND FINES
United States	• Mostly class action lawsuits • Some government enforcement actions
EU GDPR	• Fines for not notifying of a data breach can reach 2% of global turnover or €10 million, whichever is higher
Australia	• Penalty of up to AUS $2.1 million (US $1.65 million)
China	• The technical specifications are not legally binding, though failure to meet them will likely mean a breach of another law, such as the Cybersecurity Law. • For example, the Cybersecurity Law provides for fines up to RMB 500,000, closure of business and criminal prosecution.

QUESTIONS?

Lei Shen
Partner
+1 312 701 8852
lshen@mayerbrown.com

Qi Chen
Associate
+1 312 701 8735
qchen@mayerbrown.com

Oliver Yaros
Partner
+44 20 3130 3698
OYaros@mayerbrown.com

MAYER·BROWN