JP AAWG Japan Anti-Abuse Working Group

Regulatory Update

Dennis Dayman, CIPP/US, CIPP/E, CIPT, FIP

Proofpoint, Resident Chief Information Security Officer
M3AAWG, Growth & Development and Public Policy Co-Chair

Since our last visit

JPAAWG 2019

- What and why the GDPR is relevant to you in the APAC region
- Impacts from GDPR monetary fine and reputational impacts
- GDPR readiness among APAC organizations
- How you must act as a company
- Extraterritorial or cross border effects
- Ways to have lawful bases for processing of data.
- How GDPR impacts email data (use, retention, archiving processing, logs)
- The EU Adequacy Decision allowed PII to be transferred from the European Economic Area to Japan and vice verse.

- Download the 2019 PPT https://tinyurl.com/jpaawg2

Japan Act on the Protection of Personal Information (APPI)

- 2019 January 23rd
  - Japan became the first country to earn an adequacy decision from the European Commission (EC) after the GDPR came into force.
- This is the first time the E.U. and a third country have agreed on a reciprocal recognition of the adequate level of data protection.
- The mutual adequacy finding will complement the existing trade benefits of the Japan-EU Economic Partnership Agreement and contribute to the Japan-EU strategic partnership by facilitating the data flow between them.
- Companies are expected to benefit from unhindered, safe and free data transfers between the two economies that would remain restricted in the absence of the reciprocity recognition.

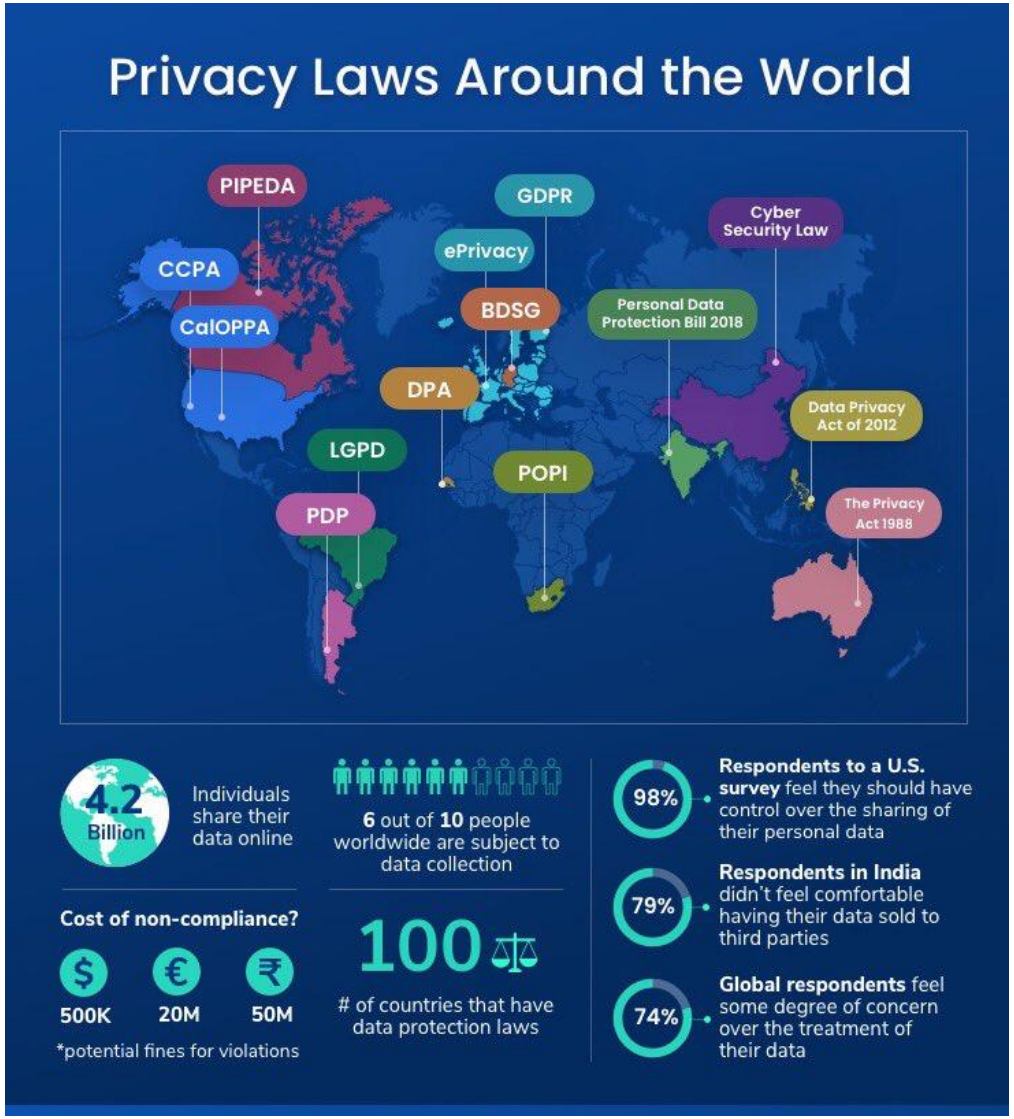
Japan Act on the Protection of Personal Information (APPI)

- APPI amendments stipulate that the law will be reviewed and updated every three years if necessary to ensure that it continues to address the latest technical developments.
  - The first such review came in 2020, and further amendments to the APPI were enacted following a public consultation on 12 June 2020.
- The new amendments brought APPI closer alignment with the GDPR by expanding the scope of Japanese data subjects' rights, making data breach notifications mandatory, and limiting the range of personal information that can be provided to third parties.
- The 2020 Amendments entered into force on 1 April 2022.

Data protection laws of the world

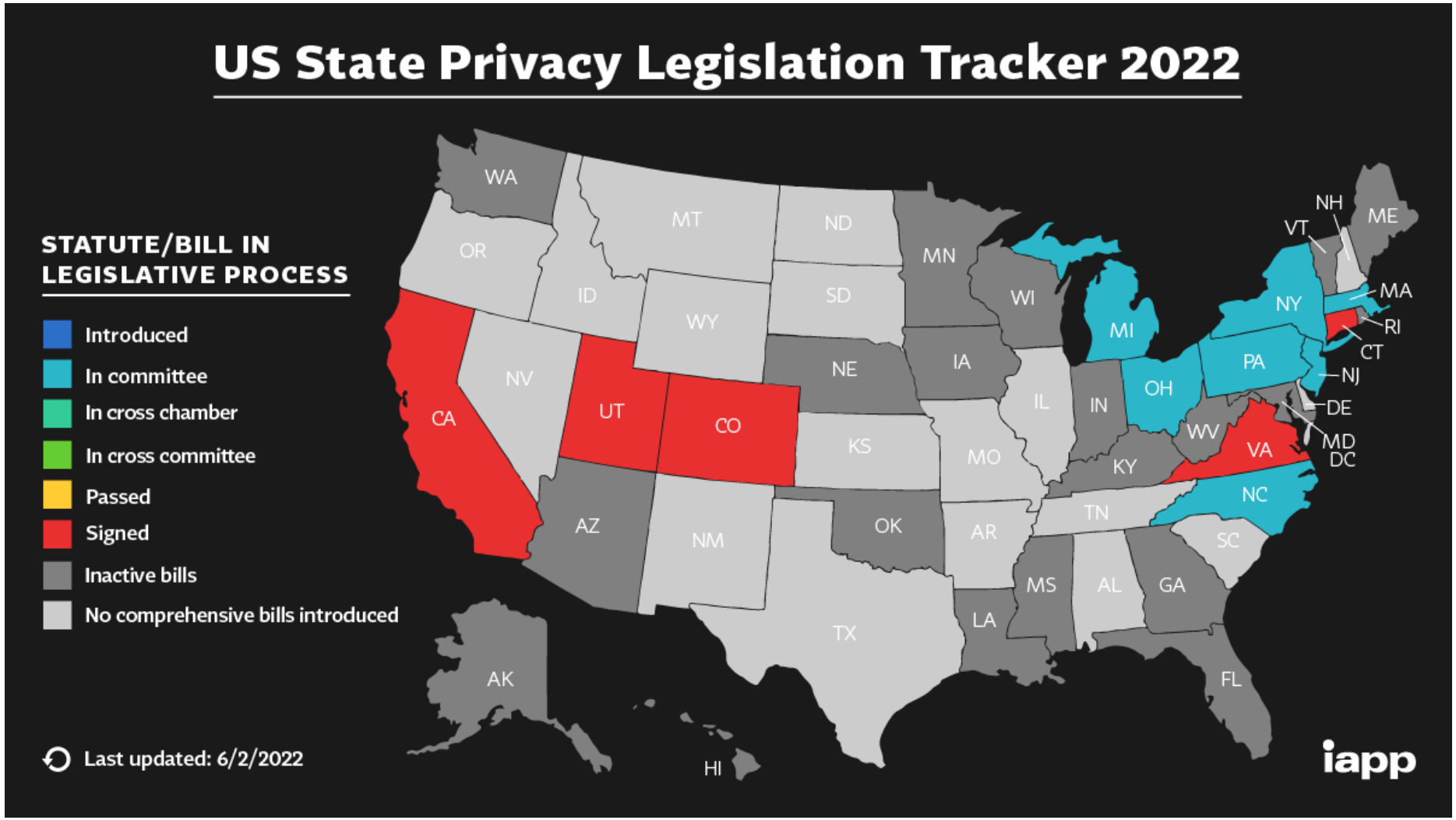
2020 became a momentous year for data protection laws around the globe

- Brazil's Lei Geral de Proteção de Dados (LGPD)
- Thailand's Personal Data Protection Act (PDPA).
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- South Korea Personal Information Protection Act (PIPA)
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)



Changes in the U.S.

U.S. State Privacy Legislation



U.S. State-level momentum for comprehensive privacy bills is at an all-time high.

Federal American Data Privacy and Protection Act (ADPPA)

- An omnibus federal privacy bill with significant bipartisan support is currently under congressional review.
- Although several other federal bills addressing PII have been introduced in recent years, the ADPPA is the first with significant bipartisan support and momentum.
- On July 20, 2022, the House Energy and Commerce Committee approved the bill by a 53-2 margin.
- The bill would create national standards and safeguards for personal information collected by companies, including protections intended to address potentially discriminatory impacts of algorithms.
- Congress is unlikely to enact the bill between now and the end of the year, but it represents progress toward a comprehensive data privacy law in the United States and is part of a growing trend calling for federal regulation.

U.S. Presidential Order

- On October 7, 2022, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which focuses on the steps the United States will take to appropriately handle European Union (EU) residents' personal information and field government surveillance complaints
- Want to establish a new EU-US Data Privacy Framework and replace the Safe Harbour/Privacy Shield.
- It addresses issues flagged by Schrems decsions that led to the downfall of the Safe Harbour/Privacy Shield

U.S. Presidential Order

- It introduces an independent and binding mechanism that would enable individuals in qualifying states and regional economic integration organizations to seek redress if they believe their personal information is collected in a manner that violates applicable US law.
- Moreover, the Executive Order introduces more safeguards for US signals intelligence activities and would require US intelligence community organizations to update their policies and procedures accordingly.
- The European Commission now will pick up the baton as it begins a ratification process that could take up to six months.

Osaka Track

JPAAWG

Data Free Flow with Trust (DFFT)

- One of the priorities set during Japan's leadership of the G20 in 2019 was the Osaka Track, a term intended to describe efforts needed across various data flow governance processes to meet this challenge.
- Prime Minister Shinzo Abe proposed the international cooperation concept of "data free flow with trust" (DFFT), a vision in which trust and openness in data flows co-exist and complement each other.
- The term suggests a wider, mutually reinforcing agenda of trade policy, regulatory and business practice cooperation, which together can create the conditions for data to flow across borders at the same time that domestic policy preferences and objectives are satisfied.

Data Free Flow with Trust (DFFT)

- Data is the fuel that powers the digital economy.
- While rules for handling data privacy and protection inevitably vary from one country to another, it is important to know we must minimize barriers to cross-border data transfers in order to address common challenges and bring benefits to society.
- A principle for rule-making in the field of cross-border data transfers.
- After its debut in Davos, DFFT was endorsed in June of 2019 by members of the G20 group of nations.

Data Free Flow with Trust (DFFT)

- What is required, then, is a pragmatic and bottom-up approach to Data Free Flow with Trust that meets the needs of business and economies.
- It was also noted that data localization requirements could lower companies' ability to ensure cybersecurity or consumer protection, and could increase entry points for cyberattacks.
- Japan's Ministry of Economy, Trade, and Industry (METI) analyzed cross-border data flows at the business level, dividing the issue into six categories of specific challenges and measures, and made recommendations.

Data Free Flow with Trust (DFFT)

Cross-border data transfers and business pain points

Types of of cross-border data transfers		Examples of Business Pain Points
1	**Product development by online app companies**	• Barriers to entry are too high for startups and SMEs as laws and regulations vary from country to country
2	**Transfer to a foreign third-country company for outsourcing**	• Unclear if data integration and data access among multiple regions across borders constitutes a "cross-border transfer" • Companies are required to ensure the same protection and management systems in the destination country as in the source country when transferring data across borders to a third country
3	**Real-time data analysis from abroad via IoT devices - no personal data is included**	• Growing regulations on non-personal data as new data categories such as "security information" emerge. Often vague in scope and prone to sudden change • Case-by-case review processes for data localization rules could undermine the advantages of real-time monitoring, a basic capability of IoT
4	**Real-time data analysis from abroad via IoT devices - personal data is included**	• "Personal data" definitions extend not only to laws but also to guidelines and administrative notices, making them difficult to implement and interpret
5	**Provide platform services and IaaS**	• Requirements for cross-border transfers are highly complex, requiring frequent customer agreement
6	**Providing cyber security services**	• Region-specific certifications may be required for security-related information, in addition to global rules and standards, imposing a significant cost burden

Where does DFFT go now?

- Despite differences in approach between the US, UK, EU, and Japan, they do share a common view that data can harness economic prosperity in a digital society and help protect is from cybercrimes.
- Ultimately the goal is to propose a set of packages to enable secure and respected cross-border free flow of data, including considerations of how it can be regulated in practice across cyber security, trade and other agreements.
- One upcoming milestone for DFFT is likely to be the G7 in 2023, which will be hosted by Japan. At Davos 2022, Japan, expressed it's commitment to the effort

Thank you for your listening!