Privacy Trends Around the World and the Implications for a Global Organization

Monday, October 22, 2018, 1:45 - 2:45 pm

Session 307

17th Annual CEI | Las Vegas

Michelle Beistle
Counsel and Chief Compliance Officer – Ethics & Privacy

Charlotte D. Young
Chief Risk and Compliance Officer

Alyssa T. Senzel
Deputy General Counsel & Compliance Officer

2

Learning Objectives

- Update on legal developments in privacy laws around the world
- Understand what trends/themes we see from these new laws
- Take away practical examples of what your entity can do right now to address these new developments and anticipate the next new law

3

The Basics: What is Privacy?

- Respect for individuals
- Protection of Personal Data
  - Personal Data = any information that identifies a specific individual
    - *Includes business contact information in many jurisdictions*
- Extra protection for personal data that can be used to cause harm

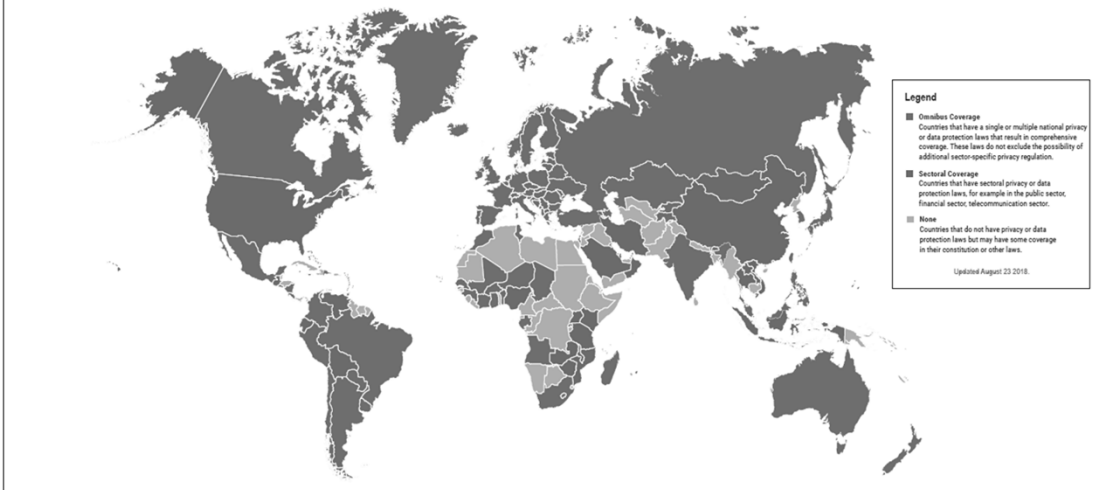
4

Compliance, Privacy, and Security

- **Compliance:** a systematic approach to governance designed to ensure that an organization meets its obligations under applicable laws, regulations, best practices, contracts, and internal policies.
- **Data Privacy**: is generally focused on the use and governance of PII. Organizations must implement policies to ensure that personal information is being collected, shared, and used in appropriate ways.
- **Data Security**: focuses on protecting data (PII, confidential information, etc.) from impermissible access, including intentional malicious attacks. Organizations maintain the privacy of their data by having security protocols in place to prevent against external threats and data breaches.

5

Sectoral and Omnibus Privacy and Data Protection Laws



NYMITY RESEARCH™

Omnibus Law Countries

Abu Dhabi, Albania, Andorra, Angola, Antigua & Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Belarus, Belgium, Benin, Bermuda, Bonaire/St. Eustatius/Saba, Bosnia & Herzegovina, Brazil, Bulgaria, Burkina Faso, Canada, Cape Verde, Cayman Islands, Chad, Chile, Colombia, Costa Rica, Cote D'Ivoire, Croatia, Curacao, Cyprus, Czech Republic, Denmark, Dominican Republic, Dubai, Estonia, Faroe Islands, Finland, France, Gabon, Germany, Georgia, Ghana, Gibraltar, Greece, Greenland, Guam, Guernsey, Guinea, Hong Kong, Hungary, Iceland, India, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Kosovo, Kyrgyz Republic, Latvia, Lesotho, Liechtenstein, Lithuania, Luxembourg, Macao SAR, Macedonia, Madagascar, Malawi, Malaysia, Mali, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Niger, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Lucia, St. Maarten, Sweden, Switzerland, Taiwan, Trinidad & Tobago, Tunisia, Turkey, Ukraine, United Kingdom, Uruguay

Sectoral Law Countries

Bahrain, Barbados, Bolivia, Bhutan, China, Ecuador, Guatemala, Indonesia, Iran, El Salvador, Jamaica, Kenya, Kuwait, Laos, Mongolia, Montserrat, Mozambique, Nigeria, Oman, Rwanda, Saudi Arabia, Tanzania, Uganda, United States, Vanuatu, Venezuela, Vietnam, Zambia

6

European Union

- General Data Protection Regulation (GDPR) went into effect May 25, 2018
  - Applies to entities collecting personal data from residents of the EEA who are residing in the EEA even if the entity does not have a presence in the EEA
  - Enforcement actions to date – mostly large social media entities and those that had to report breaches
  - Adequacy decisions underway
- ePrivacy (Regulation for Privacy and Electronic Communications) proposed January 2017 to replace ePrivacy Directive – effective ?
- NIS Directive – effective May 2018
- Privacy Shield – July 2016, annual review in Fall
- Brexit – UK Data Protection Act May 2018

7

Asia Pacific

- Australia (1988), New Zealand (1993), Hong Kong (1995) and Japan (2003) all have had comprehensive laws for many years
  - Australia did major revision in 2016 and breach notification took effect February 2018
  - Japan amendments effective in 2017 – biometrics, DPA, restrictions on cross-border
- Asia Pacific Economies Cooperation (APEC) Privacy Framework 2005
- Recent APAC countries adopting laws similar to EU = broad and comprehensive and most restrict export in some way
  - South Korea 2011; Taiwan 2012; Philippines 2012 (implemented in 2016); Malaysia 2013; Singapore 2014
  - BUT – there are differences - these are diverse countries without shared history like EU
- China Cyber Security Law – 2017 – affects data collection and processing in certain situations
- India Data Protection Bill – published August 2018

8

Latin America

- Argentina (2000), Mexico (2010), Colombia (2012), Nicaragua (2012), Uruguay (2012)
- Recent amendments make some existing laws more like EU GDPR
  - Costa Rica, amended 2016
  - Brazil August 2018 – effective February 2020
  - Peru 2017
  - Chile constitutional amendment June 2018 right to personal data protection, awaiting approval of amendment to Data Protection Act
- No specific law in El Salvador, Guatemala, Honduras
  - Draft pending in Honduras

9

United States and Canada

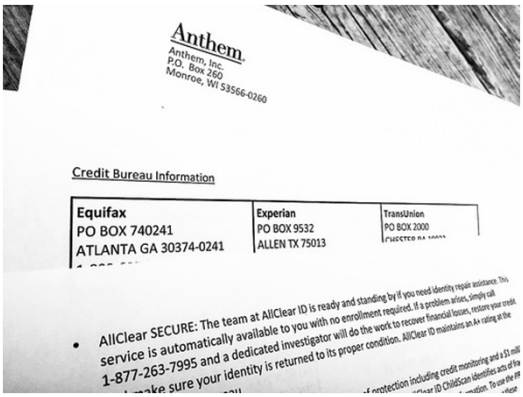
- Data Breach Notification – As of July 1, 2018 all US states have them (AL and SD were the final two)
- CA Consumer Privacy Act – June 2018, amended August 2018
  - Effective January 2020
  - Individual access rights, including erasure
  - Extra-territorial
- Canada PIPEDA (amended June 2015)
  - Canada's Anti-Spam Law (CASL) – in force July 2017
  - Breach notification effective November 1, 2018

10

What trends do we see?

Individual Rights - more transparency and control for individuals over the collection and use of their data

Breach Notification – expanded requirements for prompt reporting to authorities and individuals

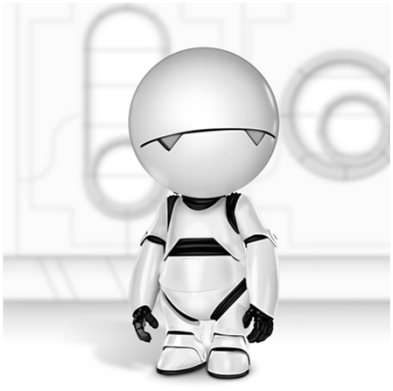


11

More trends

Limitations on transfer of personal data across borders

AI and Machine Learning – Concern about automated decision making



12

Defensible programs can mitigate fines and reputational damage

13

What does a defensible privacy program look like?

The Top 10 "Implemented" Measures

1	Maintain a data privacy policy	82.61%
2	Use contracts as a data transfer mechanism (e.g., Standard Contractual Clauses)	78.26%
3	Maintain a data privacy notice that details the organisation's personal data handling practices	76.09%
4	Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	76.09%
5	Maintain a log to track data privacy incidents/breaches	73.91%
6	Conduct privacy training	73.91%
7	Maintain procedures to respond to requests for access to personal data	71.74%
8	Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.	71.74%
9	Maintain procedures to respond to requests to opt-out of, restrict or object to processing	65.22%
10	Maintain a data privacy incident/breach response plan	65.22%

* Excerpt for 2017 Nymity GDPR Compliance Benchmarking: Measuring Accountability – survey of 190 worldwide companies and 46 EU companies across industries and of varying sizes

14

Where to begin?

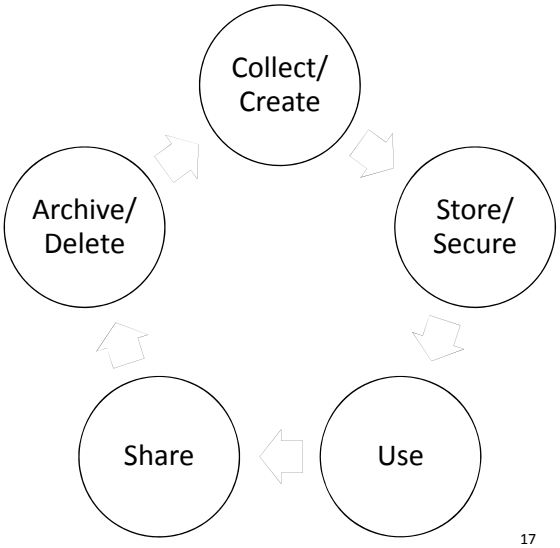
15

Prioritize

- Focus efforts on compliance with common principles across privacy laws:
  - Notice
  - Legal Basis/Consent
  - Data minimization/Retention
  - Use limitation
  - Security
  - Access & correction rights
  - Cross-border restrictions
  - Accountability & Vendor Supervision
- Prioritize:
  - High risk jurisdictions
  - High risk areas of law

16

Think about the Data Lifecycle



17

Handy Resources (Many are free!)

- Baker McKenzie Global Privacy Handbook: https://tmt.bakermckenzie.com/thought-leadership/global-privacy-handbook
- IAPP: https://www.iapp.org/ (very good free resources, paid members get more)
- Nymity: https://www.nymity.com/data-privacy-resources.aspx (very good free resources, paid subscribers get more)
- UK Information Commissioner's Office Guidance:
  - https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

18

Countries with Restrictions on Cross-Border Transfers

NYMITY RESEARCH™

Countries

Abu Dhabi, Albania, Andorra, Angola, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Belgium, Benin, Bermuda, Bonaire/St. Eustatius/Saba, Bosnia and Herzegovina, Bulgaria, Burkina Faso, Canada, Cape Verde, Cayman Islands, China, Colombia, Costa Rica, Cote D'Ivoire, Croatia, Curaçao, Cyprus, Czech Republic, Denmark, Dominican Republic, Dubai International Financial Centre, Estonia, Faroe Islands, Finland, France, Gabon, Georgia, Germany, Gibraltar, Greece, Guernsey, Hong Kong*, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Kosovo, Kyrgyz Republic, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Madagascar, Malaysia, Mali, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Norway, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, Saint Lucia, Saint Maarten, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Trinidad and Tobago, Tunisia, Turkey, Ukraine, United Kingdom, Uruguay

These countries contain restrictions around sending personal data to a third country that does not ensure an adequate level of protection.

*A commencement date for the cross-border transfers restrictions in Hong Kong has not been set yet.

19

Global Breach Response Laws

NYMITY RESEARCH™

Jurisdictions

Albania, Armenia, Argentina, Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada - Alberta - Manitoba - New Brunswick - Newfoundland and Labrador - Northwest Territories - Nova Scotia - Nunavut - Ontario - Prince Edward Island - Saskatchewan - Yukon, Cayman Islands, Colombia, Costa Rica, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Ghana, Greece, Guernsey, Hong Kong, Hungary, Ireland, Italy, Japan, Jersey, Latvia, Lithuania, Luxembourg, Malta, Mauritius, Mexico, Moldova, Netherlands, New Zealand, Norway, Peru, Philippines, Poland, Portugal, Qatar, Romania, Singapore, Slovakia, Slovenia, South Africa, South Korea (Republic of), Spain, Sweden, Taiwan, Turkey, United Arab Emirates (Dubai), United Kingdom, United States, Uruguay

This map does not reflect jurisdictions that have implemented sector-specific breach response obligations (e.g. telecoms, electronic communications providers, finance).

20