New NAFTA's Chapters 14 and 19: A Continental Privacy Regime

20th Annual Privacy and Security Conference
February 2019

Presented by:
Constantine Karbaliotis, Director
National Cybersecurity & Privacy Practice

pwc

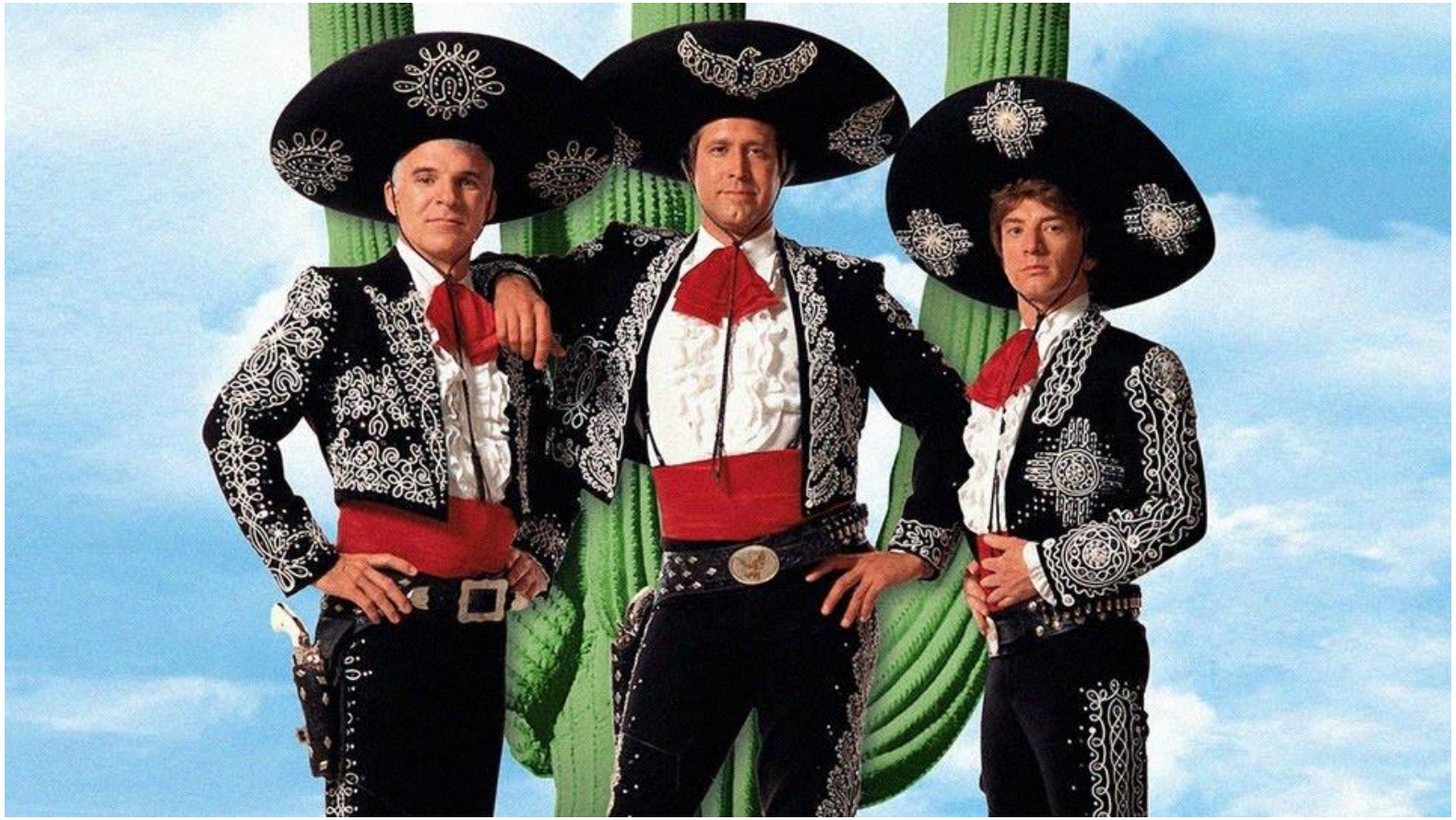
Session Description

At the end of September 2018, the US, Canada and Mexico finally concluded the New NAFTA and it has significant impact on privacy and organisations' privacy programs. The goal of the agreement is to establish free(er) trade, and Chapters 14 and 19's goal is to create a continental free trade zone in digital goods and services. The Chapter puts heavy emphasis on the countries' development of privacy regulation and collaboration in the area of personal information protection, and the use of the APEC members Privacy Framework and Cross Border Privacy Rules to support adequate data protection and cross-border data flows. Very importantly, it largely prohibits data localization requirements. PwC's privacy team (US and Canada), will discuss its provisions and how the agreement presents both challenges and opportunities to organisations operating in North America (and globally).

Take-away:

- Impact of New NAFTA on privacy
- Data localization and how it is impacted
- Leveraging the APEC Framework and CBPR for compliance

Three Amigos… Again?



The New NAFTA:

- US: USMCA
- Canada: CUSMA
- Mexico: T-MEC

New NAFTA Chapter 19 — Digital Trade

- The New NAFTA creates a continental market in digital goods and services
- Explicit requirements to ensure that personal information is protected while data localization is prohibited
- Puts onus on companies to adopt framework like APEC Privacy Framework and Cross-Border Privacy Rules and OECD Recommendations to ensure that the rules go with the data

Limitation on Data Localization

- Data localization requires that companies host and store their data within a country in order to do business there
- New NAFTA borrows general principles from the TPP in banning data localization practices
- However, New NAFTA goes even further than TPP to discourage data localization and data flow restrictions with stronger language

TPP Article 14.11(2):

Each Party **shall allow** the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

New NAFTA Article 19.11(1):

No Party **shall prohibit or restrict** the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.

Location of Processing

- New NAFTA takes language directly from TPP
- However, TPP had additional provisions, like allowing individual countries to set their own domestic requirements
- New NAFTA's position on computing facilities is more restrictive and allows for less exceptions than TPP
- New NAFTA permits government uses or procurement to be localized

TPP Article 14.13(2) + New NAFTA Article 19.12

No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

New NAFTA Article 19.3

This Chapter does not apply:
(a) to government procurement; or
(b) except for Article 19.18 (Open Government Data), to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection.

Chapter 14 — Financial Services

Canada cannot require financial institutions to use computing facilities in Canada except that OSFI or other applicable regulatory authorities:

- Must be able to have "immediate, direct, complete and ongoing access to information processed or stored on computing facilities" used by the financial institution in the United States or Mexico
- Must provide a financial institution with an opportunity to remediate a lack of access (to the extent practicable) before requiring the use of computing facilities in Canada

Chapter 14 — Financial Services Oversight

Canadian regulators can still provide oversight through:

- Requiring prior authorization to designate particular enterprises as recipients of information
- Compelling the adoption of measures relating to business continuity planning practices
- Adoption or maintenance of measures to protect personal privacy and the confidentiality of individual records and accounts

Implications for Enforcement

- Explicit but vague commitments to protect parties' consumers and their personal information
- Requires more concrete mechanisms to give effect to redress potential complaints
- CPBR could offer a useful framework for private sector, and this may presage becoming a requirement under PIPEDA or Mexico's Data Protection Law

New NAFTA Article 19.7(3):

The Parties recognize that cooperation between their respective national consumer protection agencies … is important and in the public interest. To this end, the Parties affirm that the cooperation .. includes cooperation with respect to online commercial activities.

New NAFTA Article 19.18(2):

… each Party shall adopt or maintain a legal framework that provides for the protection of the personal information … In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework…

Data Localization

- Canadian perspectives
- Mexican perspectives
- US perspectives
- A continental perspective?

New NAFTA & Privacy Regulation

- Will the 'non-discrimination' aspects of 19.11 lead to more stringent privacy regulation overall, to address concerns over the prohibition against data localization?
- How will this impact adequacy frameworks with the EU under GDPR? What challenges does this raise?

New NAFTA Article 19.11

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
2. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 necessary to achieve a legitimate public policy objective, provided that the measure:
(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

New NAFTA Article 19.14

1. Recognizing the global nature of digital trade, the Parties shall endeavor to…

(b) cooperate and maintain a dialogue on the promotion and development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes;

New NAFTA – Cybersecurity

- Does the promotion of risk management based approaches based on common standards, set a minimum expectation?

New NAFTA Article 19.15

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

New NAFTA & APEC Privacy Framework & CBPR

- Does the promotion of the APEC Privacy Framework and CBPR now set these as "baselines" for appropriate cross-border business?
- Note the note on 19.8(2): "For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy."

New NAFTA Article 19.8(2)

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

New NAFTA Article 19.8(6)

The Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

APEC in New NAFTA: A Privacy Regime to support cross-border flows

- APEC created its Cross Border Privacy Rules system (CBPR), a certification/validation and self-regulatory program that helps protect consumer data transferred within APEC economies
  - Requires participating companies to develop and implement data privacy policies consistent with the APEC Privacy Framework

- New NAFTA incorporates APEC principles; the use of the framework and formal documentation of cross-border transfers will become more important to show accountability for organisations looking to leverage the provision

Introduction to APEC and CBPR

- The Asia-Pacific Economic Cooperation (APEC) is a forum for 21 Pacific Rim member economies, which promotes free trade throughout the Asia-Pacific region
  - 12 countries acted as founding members in 1989, including the United States, Australia, Japan, and Korea
  - Membership has since grown to 21 countries

- APEC created its Cross Border Privacy Rules system (CBPR), a certification and self-regulatory program that helps protect consumer data transferred within APEC economies
  - Requires participating companies to develop and implement data privacy policies consistent with the APEC Privacy Framework
  - There are currently eight participating economies, including the United States, Mexico, Canada, Japan, and Singapore

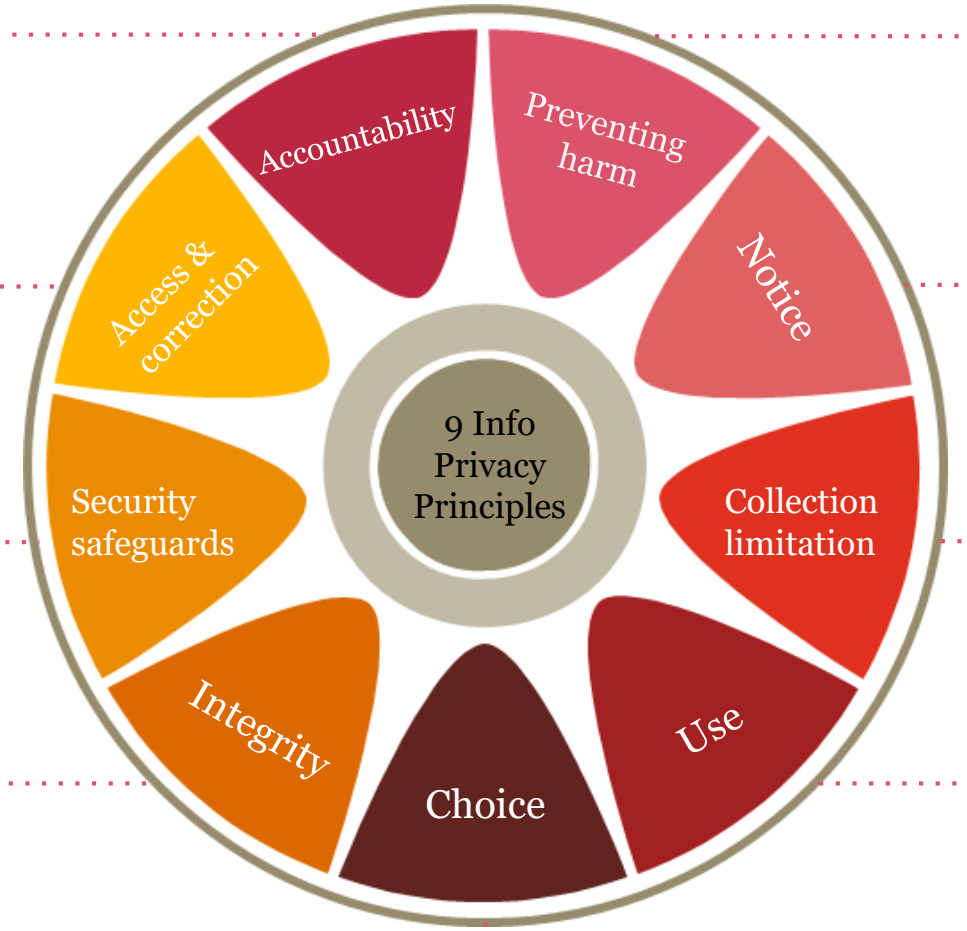
Overview of CBPR

Personal information (PI) controllers should obtain an individual's consent and exercise due diligence to properly safeguard the information.

There should be an open channel of communication between an individual and a PI controller, and the individual should be able to access and correct any of their PI.

PI controllers should safeguard PI against risks, such as loss or unauthorized access, or unauthorized destruction, use, modification, or disclosure.

PI should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.



Recognizing the interests of the individual to legitimate expectations of privacy, PI protection should be designed to prevent the misuse of such information.

PI controllers should provide clear and easily accessible statements about their PI practices and policies.

PI collection should be limited to info relevant to the collection's purposes, and any info should be fairly and legally obtained.

Generally, PI should be used only for purposes of collection and other compatible/related purposes.

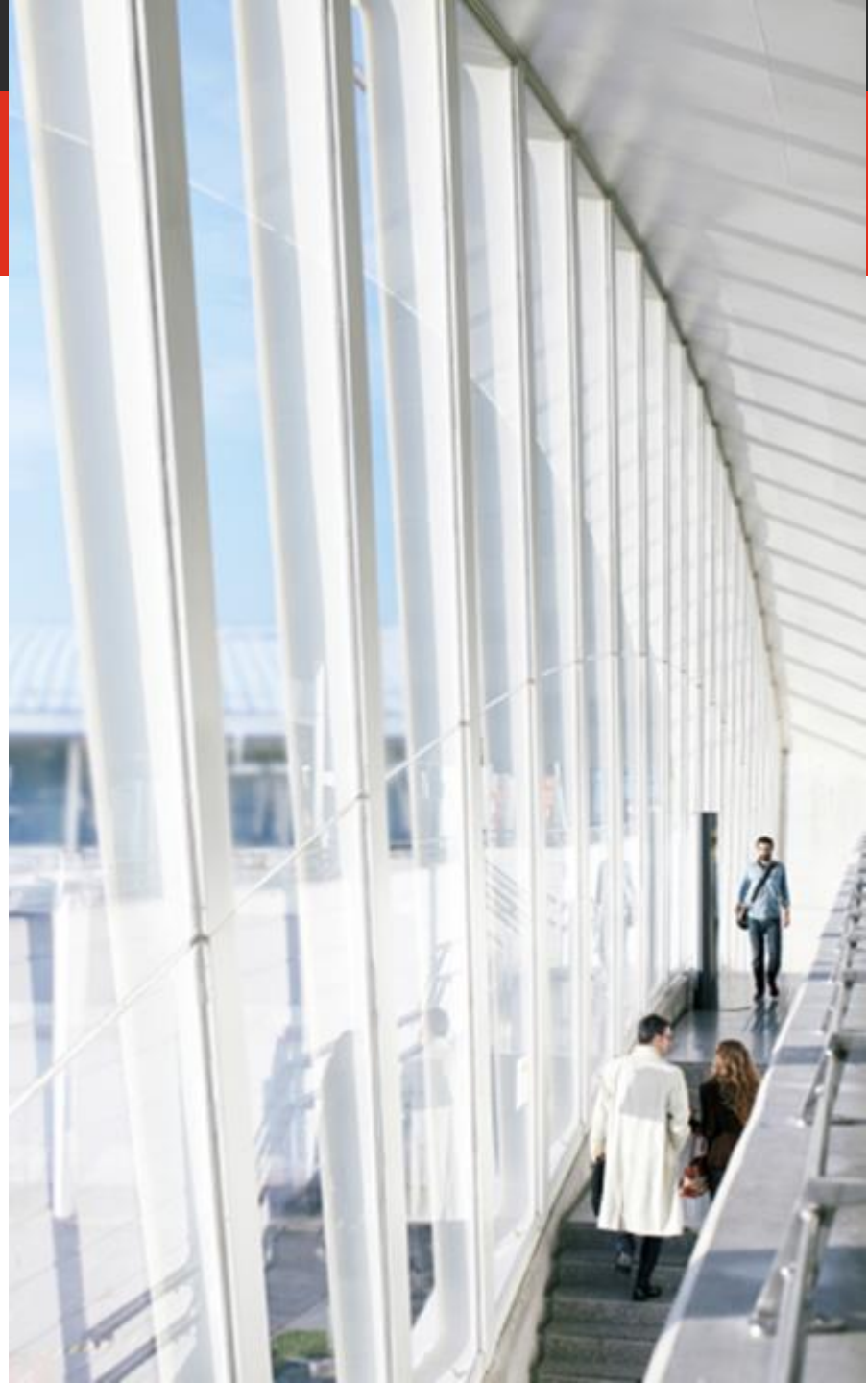
Individuals should have clear, accessible, and affordable ways to exercise choice in relation to the collection, use. and disclosure of their PI.

Update on GDPR & APEC CBPR: CBPR+?

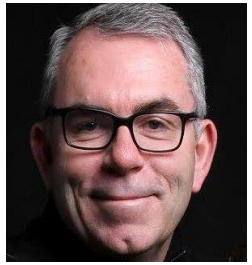
- Japan's Act on the Protection of Personal Information (APPI) was recognized as adequate by the European Commission in January 2019, the first non-Western country to attain adequacy and first under new GDPR
- Organisations in the EU can now share personal data with organisations in Japan, without needing to through the processes in Chapter 5 of GDPR
- Japanese organisations can move personal data to the EU
- Onward transfers are an ongoing concern - recognition excludes onward transfers and will be the subject of a further decision/negotiations
- Will be informative for both Canada and Mexico in retaining/attaining GDPR adequacy
- Expectation is that there will be a "CPBR+" element to address onward transfers

Conclusions & Observations

- APEC and CBPR offer a potential solutions to address consumer concerns in all three countries to ensure that the rules flow with the data:
  - A new minimum bar - information governance?
  - “Data protection, not data protectionism”
- Opportunities to integrate privacy under APEC Framework/CBPR with other regulatory frameworks – GDPR, California’s CCPA, Brazil’s LGPD – as well as enhance access to APEC itself
- Greater definition is required for enforcement and public policy-- but private sector can implement a “DIY” solution to address both consumer and regulatory expectations



Questions?



David Craig
Partner, Cybersecurity & Privacy
Email: david.craig@pwc.com
Phone: +1 416 814 5812

Jordan Prokopy
Director, National Privacy Practice Leader
Email: jordan.prokopy@pwc.com
Phone: +1 647-822-6101

Constantine Karbaliotis
Director, Leader Managed Privacy Services
Email: constantine.n.karbaliotis@pwc.com
Phone: +1 416-869-2463

Speaker

Constantine Karbaliotis– Director (Cybersecurity & Privacy)

Areas of Expertise

- Privacy
- Data Protection

Education

- J.D., Queen's University at Kingston.

Certifications

International Association of Privacy Professionals:

- Certified Information Privacy Professional – Canada, US, EU
- Certified Information Technology Professional
- Certified Information Privacy Management
- Fellow of Information Privacy

Background

Constantine is a Director of Cybersecurity & Privacy at PwC Canada and leads Privacy-as-a-Service (PraaS). He has significant privacy and consulting related expertise as demonstrated throughout his career.

An accomplished privacy professional, Constantine regularly speaks and participates internationally at privacy events. Constantine previously served as vice-president for Nymity, a leading solutions provider for privacy professionals, and before that as chief privacy officer for Mercer where he spent four years managing the company's internal compliance and the development and implementation of privacy programs, policies, and initiatives. Prior to Mercer, Constantine led the global privacy compliance program at Symantec, following his role as an executive consultant at CGI leading its privacy and security practice in Toronto. Before beginning his career in privacy, Constantine ran his own law practice. Constantine holds a J.D. from Queen's University at Kingston, Ontario and was called to the Bar of the Province of Ontario in 1986.

He brings more than 15 years of experience in the areas of international privacy and data protection (governance and policy/program development, data breach management, privacy impact assessments, vendor management, and cross-border data flows), including implementing technologies and processes for major multinationals.

His experience has included helping clients in to build effective privacy programs in Canada, the US and internationally, to remain compliant with ever-increasing expectations in privacy and data protection, and to make privacy a competitive advantage.