PCS 6166 - INTERNATIONAL DATA PROTECTION AND CYBERSECURITY LAW

Part Two – Multilateral Instruments and International Cooperation

Collaboration under PIPEDA

- Under PIPEDA (and C-11), OPC can enter into cooperation and written information-sharing arrangements with:
  - S. 23: Provincial DPAs
  - S. 23.1: Foreign bodies who have:
    - (a) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or
    - (b) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of PIPEDA.
- C-11 expands to include disclosures to CRTC / Competition Bureau

- Current international Memorandums of Understanding: Uruguay; Romania; Netherlands; Ireland; Germany; Dubai (DIFC); UK;

Canadian DPA Coordination

- Frequent joint guidance
  - See, for instance, privacy guidance on facial recognition for police agencies
- Resolutions arising from annual FPT (Federal-Provincial-Territorial) Privacy Commissioner's Conference
  - **2021**: Reinforcing privacy and access to information rights during and after a pandemic
  - **2019**: Effective privacy and access to information legislation in a data-driven society
  - **2018**: Securing trust and privacy in Canada's electoral process
  - **2017**: Safeguarding independent review of solicitor-client privilege claims
  - …
- Monthly FPT (Federal-Provincial-Territorial) calls; annual Investigators' Conference

International Collaboration / Cooperation

GDPR Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Coordinated Enforcement: Global Privacy Enforcement Network

- Arises from the OECD's Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy
- Tasks for the network:
  - Discuss the practical aspects of privacy law enforcement co-operation;
  - Share best practices in addressing cross-border challenges;
  - Work to develop shared enforcement priorities; and
  - Support joint enforcement initiatives and awareness campaigns.
- Primary output: GPEN Privacy Sweeps
  - **2020-21**: Privacy considerations and COVID-19 related solutions and initiatives
  - **2019**: Data Breach Notifications
- Also established the "GPEN Alert" network

Coordinated Policy and Enforcement: Global Privacy Assembly

- **Mission**:
  - To be a highly effective global forum for privacy and data protection authorities.
  - To provide regulatory and policy leadership at the international level in data protection and privacy.
  - To connect and support efforts at domestic and regional level, and in other international forums, to enable authorities to better protect and promote privacy and data protection.
  - To disseminate knowledge, provide practical assistance, and help authorities to more effectively perform their mandates.
  - To facilitate cooperation on cross border data flows.
- **Strategic Priorities**:
  - Advancing Global Privacy in an Age of Accelerated Digitalisation
  - Maximising the GPA's voice and influence
  - Capacity Building for the GPA and its Members

Coordinated Policy and Enforcement: Global Privacy Assembly

- Heavily focused on Resolutions
  - **2021:** Data sharing for the public good; children's digital rights; principles for governmental access to personal data held by the private sector for national security and public safety purposes
  - **2020**: Facial recognition technology; the role of personal data protection in international development aid, international humanitarian aid and crisis management; accountability in the development and use of AI; privacy and data protection challenges arising from the COVID-19 pandemic
  - **2019**: Promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement; privacy as a fundamental human right and precondition for exercising other fundamental rights; support and facilitate regulatory co-operation between DPAs and consumer protection and competition authorities; role of human error in personal data breaches; social media and violent extremist content online
- Many active working groups, including International Enforcement Cooperation Working Group (see 2021 report)
  - Key contribution: Enforcement Cooperation Handbook (updated in 2021; new version not yet available)

Other Networks

- Asia-Pacific Privacy Authorities
- Association Francophone des Autorites de Protection des Donnees Personelles
- Common Thread Network
  - Commonwealth countries
- International Working Group on Data Protection in Technology (the “Berlin Group”)
  - Focuses on developing “Working Papers”
- Network of African Data Protection Authorities

Coordinated Model Regulation: Ibero-American Data Protection Network (RIPD)

- In 2017, RIPD released its Standards for Personal Data Protection for Ibero-American States (based on GDPR)
- Specific goals:
  - To establish a set of common principles and rights for the protection of personal data which could be adopted by the Ibero-American States and develop their national legislation thereon, with the goal of having homogenous rules in the region.
  - To guarantee the effective exercise and guardianship of the right to the protection of personal data of any person in the Ibero-American States, by establishing common rules that ensure due treatment of their personal data.
  - To make the flow of personal data between Ibero-American States and beyond their borders easier, in order to contribute to the economic and social growth of the region.
  - To foster international cooperation amongst controlling authorities of the Ibero-American States, with other non-regional controlling authorities, and with international authorities and agencies in this field.
- Following this, the RIPD also issued guidance on how to comply with the Standards:
  - **2019**: General Recommendations for the Processing of Personal Data in Artificial Intelligence / Specific Guidelines for Compliance with the Principles and Rights that Govern the Protection of Personal Data in Artificial Intelligence Projects
  - **2021**: Guide on International Data Transfers (Spanish only)

Formal Coordination – European Data Protection Board

- Established / defined by Articles 68 – 76 of the GDPR
- Composed of representatives from each Member State + European Data Protection Supervisor
- 25 defined tasks, including:
  - Monitoring the correct application of the GDPR
  - Examining, on its own initiative or on request, any question covering the application of the GDPR and issue guidelines, recommendations and best practices in order to encourage consistent application;
  - Provide opinions on adequacy assessments
  - Establish requirements for certification schemes
  - Promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities

For consideration:

What if there were a Canadian Data Protection Board?

Purpose for Collaboration

- A *mea culpa* on international networks

***

- A brief case study: Netherlands' Digital Regulation Cooperation Platform
- Consists of:
  - Dutch Data Protection Authority
  - Netherlands Authority for Consumers and Markets
  - Dutch Authority for the Financial Markets
  - Dutch Media Authority
- Activities: Exchange knowledge and experiences gained from day-to-day activities; make joint investments in knowledge, experience and skills; strengthen enforcement procedures by dealing with digital market problems collectively.

Digital Regulation Cooperation Platform

- **Co-operation make regulators effective**:
  - "'A coherent and coordinated approach is needed in order to be able to respond effectively to the rapid pace of [digital] developments. That is in the interests of both users and providers of digital services."
  - "By working together, we are able to use the knowledge and expertise of our experts as effectively as possible, which is immensely beneficial."
  - "It is imperative that regulators are fully aware of where exactly the public interests that we all protect are in line with each other or perhaps conflict."
- **Enforcement crosses regulators, necessitates co-operation**:
  - "In our digital online world, protection of personal data, consumer protection, the integrity of digital content, and competition are much more intertwined than before … So the different regulators encounter each other much sooner when carrying out their duties. … Cooperation is thus of vital importance."
- **Co-operation enhances clarity and predictability**:
  - "If we collectively coordinate our oversight duties, it will also create a certain level of clarity and predictability for businesses and consumers."

See also: Global Privacy Assembly resolution on regulatory co-operation between DPAs and Consumer Protection and Competition Authorities.

Cross-border co-operation

OECD Recommendation on Cross-Border Co-operation

- Adopted in 2007
  - Development led by Jennifer Stoddart, then-Privacy Commissioner of Canada
  - Followed 2006 OECD Recommendation on Cooperation in the Enforcement of Laws against Spam
- Preface:
  - Authorities charged with enforcing privacy laws may find that they are unable to pursue complaints or conduct investigations relating to the activities of organisations outside their borders.
  - Their efforts to work together in the cross-border context may also be hampered by:
    - insufficient preventative or remedial powers
    - inconsistent legal regimes
    - practical obstacles like resource constraints

OECD Recommendation on Cross-Border Co-operation

- Recommendations:
  - That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:
    - a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.
    - b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
    - c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
    - d) Engage relevant stakeholders in discussion and activities.

OECD Recommendation – 2011 Report

- Key Activities
  - Created GPEN
  - List of national contact points for co-operation and mutual assistance
  - Request for Assistance Form
- Key Findings
  - Power to investigate is generally adequate, but further efforts needed to ensure authorities have power to administer significant sanctions
  - Legal limitations on the ability of privacy enforcement authorities to share information with foreign authorities remains an issue
  - Not all authorities set their own priorities regarding, for instance, the handling of complaints
  - Little information available re: redress for individuals in cross-border cases, or ability to use judgments obtained abroad

APEC Cooperation Arrangement for Cross-Border Privacy Enforcement

- Goals:
  - facilitate information sharing among Privacy Enforcement Authorities in APEC economies;
  - establish mechanisms to promote effective cross-border cooperation between Privacy Enforcement Authorities on the enforcement of Privacy Law, including through referrals of matters and through parallel or joint investigations or enforcement actions;
  - facilitate Privacy Enforcement Authority cooperation in enforcing Cross-Border Privacy Rules; and
  - encourage information sharing and cooperation on privacy investigation and enforcement with privacy enforcement authorities outside APEC, including by ensuring this Cooperation Arrangement can work seamlessly with similar arrangements such as those developed under the OECD Recommendation.
- Includes national contact points & request for assistance form (per OECD); also sets out process for investigative collaboration

GPA Resolution – Cross-border Enforcement

- Introduced in 2019; in full: "Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement"
- Calls upon GPA members to:
  1. Contribute knowledge and expertise to online public repository of enforcement cooperation resources;
  2. Ensure repository remains a living project;
  3. Ensure setting up the repository is streamlined;
  4. Better organize resources on GPA website;
  5. Identify legal impediments to enforcement cooperation
  6. Continue to operate a mutual observation with the OECD
  7. Update the Enforcement Cooperation Handbook and leverage lessons learned from enforcement cooperation experience.

Consistent Frameworks

OECD Framework

- 1980 Principles:
  - Collection Limitation Principle
  - Data Quality Principle
  - Purpose Specification Principle
  - Use Limitation Principle
  - Security Safeguards Principle
  - Openness Principle
  - Individual Participation Principle
  - Accountability Principle
- Updated in 2013 to include concepts such as:
  - Privacy management programmes (incl. demonstrability and breach notification)
  - Transborder data flows (incl. restrictions proportionate to risks presented, taking into account sensitivity, purpose and context)
  - National privacy strategies (incl. enforcement; support for self-regulation; adequate sanctions; education; etc.)

OECD Framework

PART SIX. **INTERNATIONAL CO OPERATION AND INTEROPERABILITY**

20.Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.

21.Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.

22.Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

23.Member countries should make public the details of their observance of these Guidelines.

OECD Framework

- 2021: Second Report on Implementation of the OECD Framework
- Key takeaways:
  - Framework remains an important baseline
  - However, modern digital economies and data-centric technology is challenging the application of the Principles
  - Areas where additional guidance is needed on:
    - Implementation of accountability (i.e. accountability as compliance with legal obligations requires evolution)
    - Need to "further examine good practices among Adherents concerning 'guarantees' or 'restraints' on government access to data held by the private sector to ensure trust in data flows."
    - Additional data subject rights (data portability; correction and erasure; right to object to automated decision-making)
  - Further analytical work requests on regulatory sandboxes, certification schemes, transparency reporting, privacy enhancing technologies
  - Support for "Cross-cutting work to identify intersections between privacy, consumer and competition policy, and stronger co-operation between different types of regulators, as well as on cross-border co-operation in the enforcement of laws protecting privacy"

APEC Framework

"APEC member economies realize the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A framework to enable regional data transfers will benefit consumers, businesses, and governments"

OECD Framework	APEC Information Privacy Principles
Collection Limitation Principle	Preventing Harm
Data Quality Principle	Notice
Purpose Specification Principle	Collection Limitation
Use Limitation Principle	Use of Personal Information
Security Safeguards Principle	Choice
Openness Principle	Integrity of Personal Information
Individual Participation Principle	Security Safeguards
Accountability Principle	Access and Correction
	Accountability

APEC Framework

Preventing Harm Principle:

"Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information."

Commentary:

"The Preventing Harm Principle recognizes that **one of the primary objectives of the APEC Privacy Framework is to prevent misuse of personal information and consequent harm to individuals**. Therefore, privacy protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, **remedies for privacy infringements** should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and **should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information**.

OECD Framework - Purpose

- RECOGNISING that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;
- RECOGNISING that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;
- RECOGNISING that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;
- RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy;
- RECOGNISING the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;
- DETERMINED to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them;

APEC Framework

APEC Framework was developed in recognition of the importance of:

- Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;
- Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- Enabling enforcement agencies to fulfill their mandate to protect information privacy;
- Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

Global Privacy Assembly

- 2019: Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights
  - Sponsored by OPC-Canada
- Calls to Action:
  - Government: Recognize privacy as a fundamental human right, vital to the protection of other human rights
  - Legislators: Review and update privacy and data protection laws
  - Regulators: Apply all relevant laws to activities of all actors in the political ecosystem
  - Businesses: Show demonstrable accountability
  - Civil society, media and citizens: Exert privacy rights by openly voicing concerns
  - All organizations: Assess risks to rights before using artificial intelligence

Declaration on European Digital Rights

- Released January 26, 2022
- The Declaration should:
  - Serve as a reference for both public and private actors when developing and deploying new technology
  - Guide policy makers in a joint effort to define the European way to a sustainable, human-centred, inclusive digital world, and to firmly anchor EU policy interventions to that end.
- Preamble:
  - The digital transformation affects every aspect of people's lives. It offers significant opportunities for a better quality of life, innovation, economic growth and sustainability, but it also presents new challenges for the fabric, security and stability of our societies and economies. With the acceleration of the digital transformation, the time has come for the European Union (EU) to spell out how its values and fundamental rights should be applied in the online world.

Declaration on European Digital Rights

On privacy and cybersecurity:

A protected, safe and secure online environment

Everyone should have access to digital technologies, products and services that are safe, secure, and privacy-protective by design.

We commit to:

- protecting the interests of people, businesses and public institutions against cybercrime, including data breaches and cyberattacks. This includes protecting digital identity from identity theft or manipulation.
- countering and holding accountable those that seek to undermine security online and the integrity of the Europeans' online environment or that promote violence and hatred through digital means.

Privacy and individual control over data

Everyone has the right to the protection of their personal data online. That right includes the control on how the data are used and with whom they are shared. Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and no one shall be subjected to unlawful online surveillance or interception measures. Everyone should be able to determine their digital legacy, and decide what happens with the publicly available information that concerns them, after their death.

We commit to:

- ensuring the possibility to easily move personal data between different digital services.

United Nations – The right to privacy in the digital age

- Most Recent Resolution adopted on December 16, 2020 (previous similar resolutions in, 2018, 2016, 2013)
- Preamble (from 2018):
  - Noting that the **rapid pace of technological development enables individuals all over the world to use new information and communications technologies** and at the same time **enhances the capacity of Governments, companies and individuals to undertake surveillance, interception and data collection**, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,
  - Noting also that **violations and abuses of the right to privacy in the digital age may affect all individuals**, with **particular effects on women, as well as children and those who are vulnerable and marginalized**,
  - Recognizing that the promotion of and **respect for the right to privacy are important to the prevention of violence**, including gender-based violence, abuse and sexual harassment, **in particular against women and children, which can occur in digital and online spaces and includes cyberbullying and cyberstalking**,
  - Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and **recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society** …

United Nations – The right to privacy in the digital age (cont'd)

- Preamble (cont'd):
  - Noting that, while metadata may provide benefits, **certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications** and can give an insight into an individual's behaviour, social relationships, private preferences and identity,
  - Expressing concern that **individuals often do not and/or cannot provide their free, explicit and informed consent** to the sale or multiple resale of their personal data, as the collecting, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age,
  - Noting with concern that profiling, automated decision-making and machinelearning technologies, sometimes referred to as **artificial intelligence, without proper safeguards, may lead to decisions that have the potential to affect the enjoyment of human rights**, including economic, social and cultural rights, and recognizing the need to apply international human rights law in the design, evaluation and regulation of these practices,

United Nations – The right to privacy in the digital age (cont'd)

- Resolution – The UN General Assembly:
- Calls upon States to:
  - Respect the right to privacy;
  - Take measures to put and end to violations of the right to privacy;
  - To review their surveillance practices (and associated legislation)
  - To establish or maintain independent, effective and adequately resourced DPAs
  - To provide individuals whose privacy is violated with access to an effective remedy
  - To *consider* developing or maintaining adequate legislation that protects individuals against violations / data protection legislation
  - …
  - To provide effective guidance to business enterprises on how to respect human rights
  - To promote quality digital literacy education
  - …
- Calls upon businesses to:
  - Meet their human rights responsibilities; provide notice of c/u/d; implement safeguards; design human rights protection into ADM
    …

Human Rights Frameworks

- UN Universal Declaration of Human Rights / International Covenant on Civil and Political Rights
  - Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- Same basic text in:
  - International Covenant on Civil and Political Rights, Article 17
  - Convention on the Rights of the Child, Article 16
  - International Convention on the Protection of All Migrant Workers and Members of Their Families, Article 14
- See UN OHCHR page on Privacy and International Standards
- See also: Teresa Scassa's A Human Rights-based Approach to Data Protection in Canada

A human rights-centric preamble?

- …
- Considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data;
- Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;
- …
- Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people;

Convention 108+

- Convention 108 developed by Council of Europe in 1980, amended in 2001
  - Ratification: All 47 members of Council of Europe; Argentina; Cabo Verde; Mauritius; Mexico; Morocco; Senegal; Tunisia; Uruguay
- Convention 108+ introduced in 2018
  - Full list of "novelties" in Convention 108+
  - Ratification: 14 members of CoE (40 of 47 are signatories); Mauritius; Uruguay (Argentina and Tunisia are signatories)
- Only binding international convention within privacy and data protection

---

- Purpose: "to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy."

Convention 108+ (cont'd)

- 5 - Focus on proportionality and fairness
  - Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.
- 6 - Specific safeguards required for sensitive information
  - The processing of genetic data, data related to offenses, identifying biometric data, and personal data related to racial / ethnic origin, political opinion, religious belief, etc. shall only be allowed where appropriate safeguards are enshrined in law
  - Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.
- 9 - Data subject rights
  - Right not to be subject to ADM without having views taken into consideration
  - Right to request access / descriptions of processing;
  - Right to request reasoning underlying processing;
  - Right to object
  - Right to request rectification / deletion
  - Right to remedy
  - Right to assistance regardless of nationality or residence

Convention 108+ (cont'd)

- 10.2 – Requirement that controllers examine likely impact on rights and freedoms
- 11.1 – Law enforcement exceptions must "respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society"
- 14 - Transborder Data Flows
  - A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention
  - If transfer is to a party not subject to the Convention, appropriate level of protection is required.
- 15 – Supervisory authorities shall have the powers to issue decisions and may impose administrative sanctions.
  - 15.3: The competent supervisory authorities **shall** be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

Convention 108+ (cont'd)

- Regulatory cooperation:
  - The supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by:
    - providing mutual assistance by exchanging relevant and useful information and co-operating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with;
    - co-ordinating their investigations or interventions, or conducting joint actions
    - providing information and documentation on their law and administrative practice relating to data protection.
- …
  - In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.
- In general, DPAs cannot refuse co-operation requests. (Article 20)

Convention 108+ cont'd

- Benefits to non-CoE Nations' accession to Convention (Greenleaf *via* Bennett):
  - Signals a recognition of best practices
  - Can serve as an alternative to the specification of "whitelists" for data exports
  - Assists in the determination of adequacy under the GDPR
  - May assist certain international organizations in areas such as policing, financial surveillance, and humanitarian assistance that must develop procedures for international transfers of personal data
  - Facilitates assistance between DPAs
  - Provides certain benefits for businesses, both exporters and importers, and data controllers and data processors, where there are reciprocal obligations
  - Provides benefits for individual data subjects, because enforceable privacy laws apply wherever their data is exported, and DPAs are required to aid these individuals

Convention 108+ cont'd

- Benefits of ratification for Canada (per Bennett):
  - Enhance Canada's likelihood of extending its adequacy status
  - Establishes a safe harbor with multiple non-EU countries
  - Saves the need for politically-sensitive adequacy decisions
  - Helps resolves inconsistencies within Canada (at least re: partial adequacy)
  - Could permit cross-border protections not permitted under trade agreements
  - Remedies some weaknesses in CBPR system

Cybersecurity Co-operation

- 2015 UN Group of Government Experts Report
  - Builds on 2013 report
- "Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. … Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development."
- GGE Report norms include:
  - States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
  - States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats;
  - A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
  - States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams
  - …

Cybersecurity Co-operation (cont'd)

- … and "confidence building measures"
  - The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations
  - Encouraging transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work
  - The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders.
  - …

(Purpose: "to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.")

Cybersecurity Co-operation (cont'd)

- UN's confidence-building measures complemented in similar documents from orgs such as the Organization for Security and Co-operation in Europe

- See also regional agreements such as the ASEAN-EU Statement on Cybersecurity Cooperation; Canada-US Cybersecurity Action Plan

Data Sharing Instruments

APEC CBPRs

- Voluntary, accountability-based system that facilitates data flows among APEC companies
- Main components:
  - Recognition criteria for organisations wishing to become an APEC CBPR System certified Accountability Agent
  - Intake questionnaire for organisations that wish to be certified as APEC CBPR System compliant by a third-party CBPR system certified Accountability Agent
  - Assessment criteria for use by APEC CBPR System certified Accountability Agents when reviewing an organisation's answers to the intake questionnaire
  - A regulatory cooperative arrangement (the CPEA) to ensure that each of the APEC CBPR system program requirements can be enforced by participating APEC economies.
- Also developed "Privacy Recognition for Processors" program
- Current members:
  - Australia, Canada, Chinese Taipei, Japan, Mexico, Philippines, Singapore, South Korea, United States
- Accountability agents available in Japan, Korea, Singapore, United States, Chinese Taipei

APEC CBPRs (cont'd)

- **Enforceable standards**: To join, participating economies must demonstrate that CBPR program requirements will be legally enforceable against certified companies.
- **Accountability**: To become certified, a company must demonstrate to an Accountability Agent—an independent CBPR System-recognized public or private sector entity— that they meet the CBPR program requirements, and the company is subject to ongoing monitoring and enforcement.
- **Risk-based protections**: Certified companies must implement security safeguards for personal data that are proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held.
- **Consumer-friendly complaint handling**: Accountability Agents receive and investigate complaints and resolve disputes between consumers and certified companies in relation to non-compliance with its program requirements.
- **Consumer empowerment**: Certified companies must provide consumers with the opportunity to access and correct their personal data. Further, by publicly certifying to the CBPR System's requirements, consumers gain insight into the privacy practices on business with which they choose to do business.
- **Consistent protections**: While governments may impose additional requirements with which certified companies must still comply, all participants must agree to abide by the 50 CBPR program requirements, facilitating the implementation of the same baseline protections across different legal regimes.
- **Cross-border enforcement cooperation**: The CBPR System provides a mechanism for regulatory authorities to cooperate on the enforcement of program requirements.

(via What is the Cross-Border Privacy Rules System)

APEC CBPRs (cont'd)

- Recognized in the Canada-US-Mexico Agreement ("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).

  - 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.

EU Standard Contractual Clauses (SCCs)

- GDPR Article 46: Transfers subject to appropriate safeguards
  - 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
  - 46(2): The appropriate safeguards referred to in paragraph 1 may be provided for by:
    - (c) standard data protection clauses adopted by the Commission;
    - (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission;

- Two versions (updated in June 2021):
  - Standard contractual clauses for controllers and processors
  - Standard contractual clauses for international transfers

Canada – US Data Sharing Instruments

- “Beyond the Border Action Plan”

  -> Canada-U.S. Border Information Sharing Treaty

  -> Joint Statement of Privacy Principles

- US Foreign Account Tax Compliance Act

  -> Canada-US Enhanced Tax Information Exchange Agreement

The Broken Instruments – Safe Harbor

- In 2000, EU Commission and US Government created the "EU-US Safe Harbor Framework"
- In short, US companies had to self-certify that they comply with seven principles related to:
  - Notice
  - Choice
  - Onward transfer
  - Access
  - Security
  - Data integrity
  - Enforcement
- European Commission deemed EU-US Safe Harbor regime "adequate"

(A reminder on adequacy: Under EU DPD and GDPR, transfers of personal data to third countries *or international organizations* do not require any specific authorization if the recipient "ensures an adequate level of protection." See GDPR Article 45)

- 2015: Max Schrems argues that Snowden Revelations prove that Facebook data transferred from Ireland to US is accessible by US intelligence authorities, violating EU data protection rights. CJEU agrees, overturns adequacy ruling. ("Schrems I")

The Broken Instruments – Privacy Shield

- Post Schrems I, new agreement rapidly drafted. Initial draft was insufficient, but as amended was granted adequacy status in June 2016.
- July 2020: Adequacy decision again struck down due to insufficient protection against US government surveillance. (“Schrems II”)

- Doesn’t explicitly prohibit transfers based SCCs, but leaves open the possibility that they are also insufficiently protective.
  - Requires es and regulators to conduct case-by-case analyses to determine whether foreign protections concerning government access to data transferred meet EU standards.

The Role of Civil Society

- Max Schrems and NOYB
  - Responsible for demise of Safe Harbor ("Schrems I"), Privacy Shield ("Schrems II"),
  - More recently, the "101 US Transfer Complaints" against companies in all 30 EU and EEA member states
    - Decision 1: Austria
    - Decision 2: France
    - NYOB's "long-term solution": Either the US adapts baseline protections for foreigners to support their tech industry, or US providers will have to host foreign data outside of the United States.
- Johnny Ryan (formerly of Brave; now of Irish Council for Civil Liberties)
  - Active campaigner against "Real-Time Bidding"; GDPR complaints filed in UK and Ireland in 2018; others in 2019
  - Belgian finding against IAB Europe is direct result

In Canada?

- Citizen Lab
  - Access My Info tool had major compliance impacts
  - Playbook has been developed to allow for replication

End Part 2.