CROSS-BORDER & INTERNATIONAL DATA PRIVACY ISSUES

BRENT ARNOLD, TODD BURKE

March 16, 2021

GOWLING WLG

LEGAL DISCLAIMER

- The presentation today is not intended as legal advice.
- Because this is a high level overview, it is impossible to cover all relevant details, and your available rights and remedies will depend on the unique facts of each situation, your applicable contract or subcontract, or the nature of your project.
- For specific advice, please contact your qualified legal counsel before making any decisions or taking any action. This is of particular importance as every province and territory has its own legal regime.
- As you know, the situation is extremely fluid and is changing on a daily basis. As things evolve, your best course of action could also evolve. Please follow up to date and reliable sources for your information.

AGENDA

Topic
Changes in U.S. Law
Europe, the GDPR, and *Schrems II*
Canada
China
Recommendations
Questions?

UNITED STATES

***California Privacy Rights Act* (CPRA), November 2020:**

- Expanded the *California Consumer Privacy Act* (CCPA)
- **Adds new "Sensitive Data"** category including social security numbers, financial account information, login credentials, geolocation information and information that exposes genetics, racial or ethnic origin, religious beliefs, biometrics, health data, sex life and sexual orientation
- No GDPR-style consent obligation, but **greater control for data subjects over their own data**
- **New definition of consent** (any freely given, specific, informed[,] and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose.")

UNITED STATES

***California Privacy Rights Act* (CPRA), November 2020:**

- Expands CCPA requirements re: privacy provisions required for contracts with service providers, **which must now prohibit:**
  1. Sale / sharing of personal information
  2. Retention / use / disclosure except for purposes specified in contract
  3. Combining data with data received from others

GOWLING WLG

UNITED STATES

***California Privacy Rights Act* (CPRA), November 2020:**

- **Contracts must also specify that:**
  1. Personal info sold / disclosed by service provider is “only for limited and specific purposes”
  2. **The service provider is subject to the CPRA and must provide the protections it requires**
  3. The transferor retains the right to take “reasonable and appropriate steps” to ensure CPRA compliance by the service provider
  4. **The service provider must provide notify the transferor that it can’t meet its CPRA obligations**
- **The Act includes a private right of action**

UNITED STATES

New privacy laws?

- IAPP expects changes in California law, along with the coming in of a new administration, and the convergence of Democratic and Republican party positions over a new, comprehensive federal law to result in such a law, perhaps this year

- Business Insider predicts that industry group pressure for a rationalization and clarity of U.S. federal privacy law

UNITED STATES

New privacy laws?

- Washington State is attempting(again) to pass a CCPA/CPRA-style *Washington Privacy Act* (WPA); passed by the state Senate for a third time March 2021;now moves to the House of Representatives
- Similar bills introduced in 20 states so far
- Virginia enacted a similar bill, signed into law March 2, 2021 (takes effect January 1, 2023)

UNITED STATES

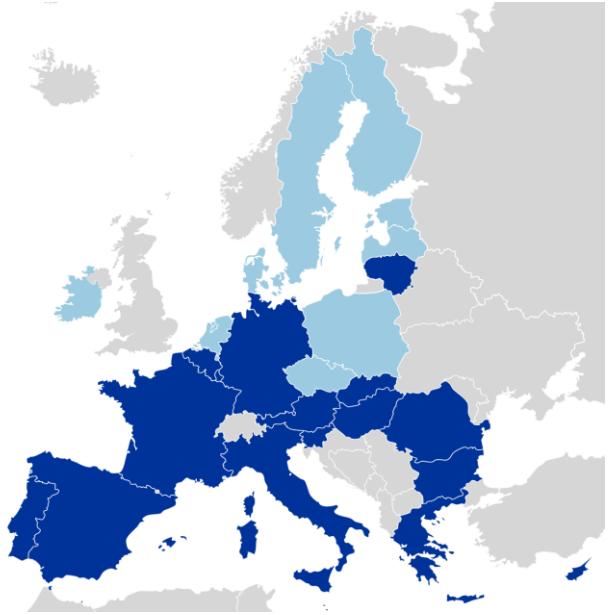
New privacy laws?

- **Bills working through legislative process** in Oklahoma, Connecticut, Florida, Illinois
- **Bills introduced** in Alabama, Arizona, Kentucky, Maryland, Massachusetts, Minnesota, New York, Rhode Island, South Carolina, Texas, Vermont
- **Bills DOA** in North Dakota, Mississippi and Utah

GOWLING WLG

EUROPE—DATA GOVERNANCE ACT

- European Commission released draft *Data Governance Act* in November 2020
- Intended to give EU a competitive advantage by increasing the safe sharing of public sector data between members
- Would allow EU-wide data sharing in strategic sectors (energy, health)
- Includes special rules for cross-border transfers of “highly sensitive” but non-personal data, and of data protected by IP rights

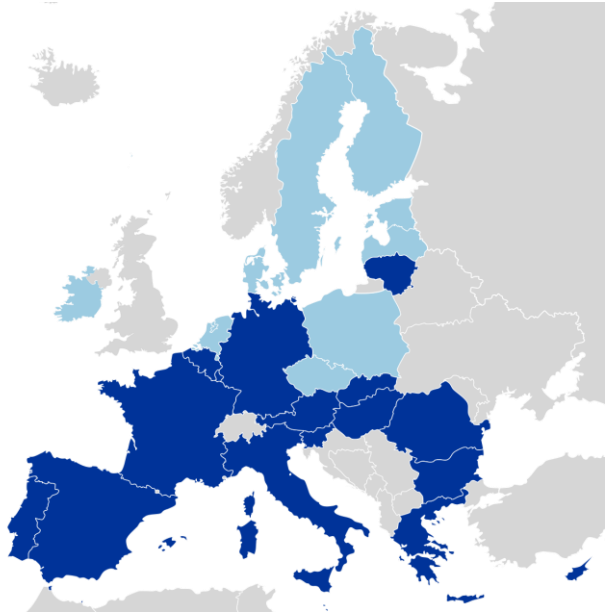


GOWLING WLG

EUROPE—NEW EDPB GDPR STRATEGY

New European Data Protection Board (EDPB) GDPR Strategy 2021-2023 published 5 January 2021:

- Gaps, differences in national enforcement procedures of member states slows down progress of cross-border protection cases
- EDPB plans to strengthen cooperation between national supervisory authorities by **streamlining processes and implementing Coordinated Enforcement Network** to ensure cooperation
- May also establish a “Support Pool of Experts” to share expertise for investigation and enforcement

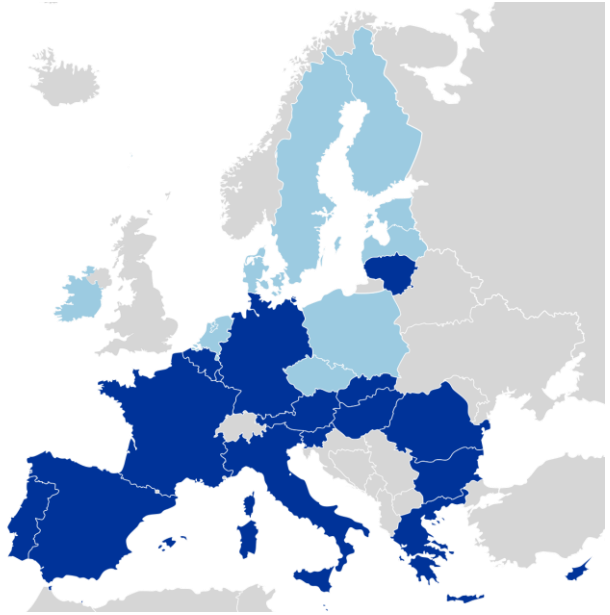


GOWLING WLG

EUROPE—NEW EDPB GDPR STRATEGY

What it means for you:*

- Data controllers, processers should **monitor EDPB's new guideline and future statements** / opinions re: data subject rights
- **National authorities within the EU will be acting together** to issue joint actions, investigations, procedures to enhance competition and consumer protection
- Cross-border enforcement (within Europe) should become faster
- **Guidance on international data transfers** (i.e. between EU and the rest of the world) are likely on the way



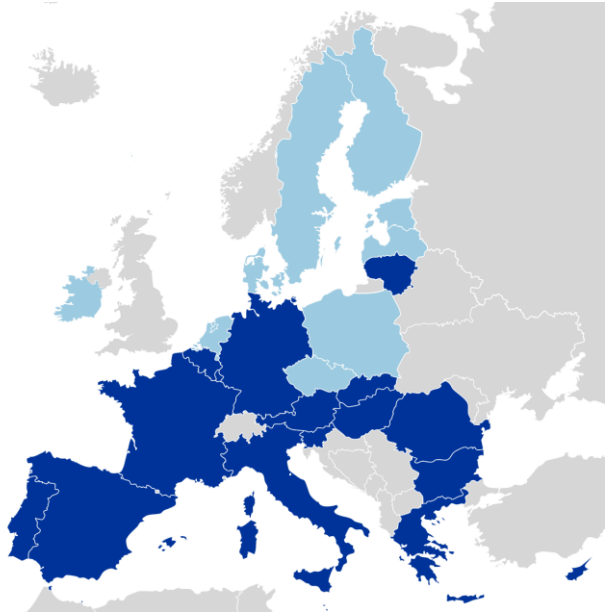
*Sources: CMS Cameron McKenna Nabarro Olswang LLP, https://www.cms-lawnow.com/ealerts/2021/01/new-gdpr-strategy-to-tackle-new-technology-data-security-international-data-transfers?cc_lang=en

GOWLING WLG

SCHREMS II

***Schrems II* ruling by the Court of Justice of the European Union (CJEU), 16 July 2020:**

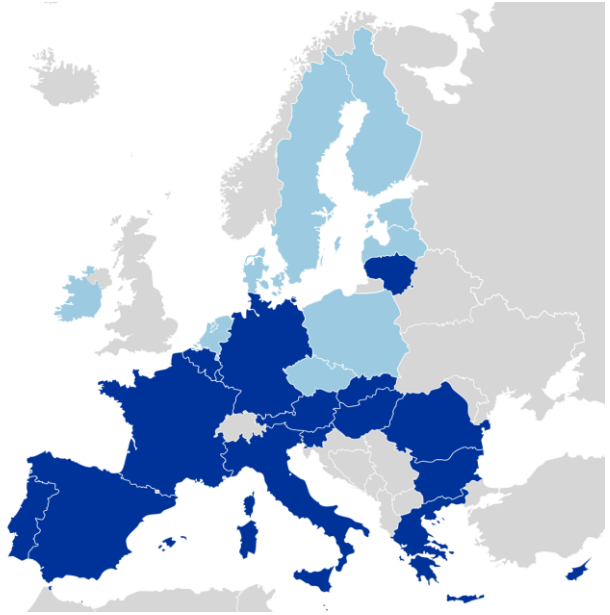
- Court found in favour of privacy activist Maximillian Schrems, challenging transfer of data by Facebook from Europe to its U.S. entity
- Prior to the court challenge, data controllers processors could rely on the Privacy Shield Transatlantic treaty covering data transfers
- **The Shield allowed companies to transfer data without having to independently verify the adequacy of the privacy regime in the recipient state**



GOWLING WLG

SCHREMS II

- Decision invalidated the Treaty, finding U.S. privacy measures insufficiently comparable to the GDPR (because data subjects' rights weren't actionable against U.S. authorities in U.S. courts)
- **Companies must now independently ensure data in the recipient state will have protection at a level comparable to EU / EEA**
- Possible measures to achieve this include standard contract clauses, binding corporate rules, codes of conduct, certification measures



GOWLING WLG

SCHREMS II—GUIDANCE FROM EUROPEAN DATA PROTECTION BOARD (EPDB)

EPDB published guidance on *Schrems II,* November 2020:

- Recommends measures to supplement transfer tools to ensure GDPR compliance
- **Transfer compliance**: Data exporter must be able to confirm data transferred complies with GDPR (i.e. as limited as possible in scope, relevant, and adequate)
- **Transfer tool verification:** Where no adequacy decision exists, rely on one of the tools in GDPR Articles 46 and 49
- **Assess third party country law's effect:** Transferor must assess whether third country (recipient country) laws will lessen the protective power of the transfer mechanism (e.g. third party country laws permit greater access, retention or use of the data by third country public authorities than is compatible with GDPR)

SCHREMS II—GUIDANCE FROM EUROPEAN DATA PROTECTION BOARD (EPDB)

EPDB published guidance on *Schrems II*, November 2020:

- **Identify, adopt supplementary measures**: Where laws of third party country impinge one effect of the transfer tool, transferor must adopt additional measures to bring the third country's data protection back up to EU standard (measures may be chosen from an annex of suggestions including hashing and encryption)

WHAT ABOUT BREXIT?

Trade and Cooperation Agreement, in effect January 2021 (formal adoption February 2021):

- Allows EU, UK to develop, adopt different data protection measures, including in re: data transfers
- Transfers of personal data from the EEA to UK will = transfer to a "third country," requiring GDPR Article 46 standards (e.g. standard contractual clauses, binding corporate rules)

GOWLING WLG

WHAT ABOUT BREXIT?

Trade and Cooperation Agreement, in effect January 2021 (formal adoption February 2021):

- UK becomes “third country” as soon as (i) ECC adopts an adequacy decision re UK privacy regime, or (ii) April 30, 2021
- Two draft adequacy decisions were under consideration as of mid-Feb 2021 and await opinions from the European Data Protection Board

GOWLING WLG

WHAT ABOUT BREXIT?

Trade and Cooperation Agreement, in effect January 2021 (formal adoption February 2021):

- UK has deemed EU / EEA states to be “adequate” on transitional basis pending review, so for now, alternative transfer mechanisms such as standard contract clauses aren’t required
- UK has agreed to uninterrupted data transfers with Argentina, Canada, Japan, New Zealand, Switzerland, and a few others; others will require binding corporate rules
- **UK no longer part of the GDPR One-Stop-Shop mechanism**

CANADA

- Provinces are either under federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) or substantially similar legislation

- Statute, regulations don't expressly require additional consent to share / transfer data across organizations / borders

GOWLING WLG

CANADA

Federal Office of the Privacy Commissioner's stance since 2009:*

1. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing.
2. PIPEDA does establish rules governing transfers for processing.
3. A transfer for processing is a "use" of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required.

*Source: OPC, Guidelines for Processing Personal Data Across Borders, https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

GOWLING WLG

CANADA

Federal Office of the Privacy Commissioner public consultation in 2019:

- Considered whether prior consent is required for all disclosures of info between individuals, including transfers between organizations and their service providers. This would have include transfers within Canada or cross-border

- Proposal *expressly* contemplated obligation to obtain express prior consent to disclosure across a border

- Aborted following the release of the Federal *Digital Charter* with and announcement of overhaul of federal privacy laws

GOWLING WLG

CANADA

Bill C-11, the *Digital Charter Implementation Act*, 2020 (DCIA)

- Cross-border transfers still permitted
- **Like PIPEDA, oes not distinguish between domestic and international transfers of personal information or impose specific restrictions on cross-border transfers**
- Organizations may transfer data for processing without data subject knowledge or consent

CANADA

Bill C-11, the *Digital Charter Implementation Act*, 2020 (DCIA)

- Allows transfer of personal data to a "service provider" (including one outside Canada), defined as "an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, which provides services for or on behalf of another organization to assist the organization in fulfilling its purpose" (s.2)
- **Introduces a private right of action → likely to fuel new class actions for violations**

CANADA

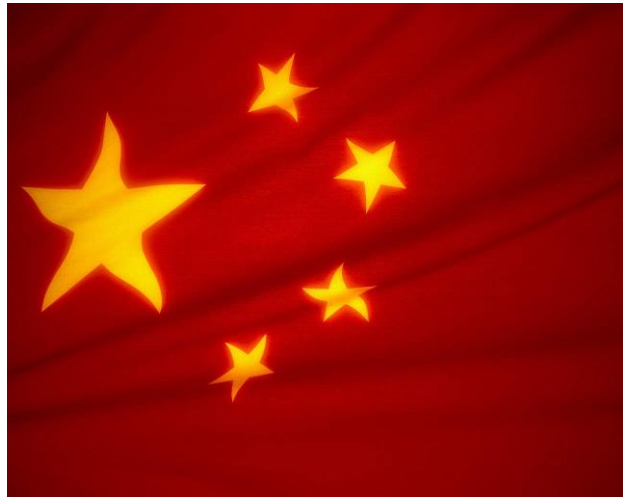
Bill C-11, the *Digital Charter Implementation Act*, 2020 (DCIA)

- Organizations may transfer data for processing without data subject's knowledge or consent
- Bill clarifies accountability issues:
  - Personal info gathered by service provider on behalf of the transferor is deemed to be under the control of the transferor, not the service provider, if the transferor is responsible for determining the purpose of the collection / use / disclosure by the service provider (s.7(2))
  - Transferor is responsible for to ensure CPPA-compliant protection of the transferred info (s.11(1));
  - CPPA's obligations don't apply to service provider *unless* it collects / uses / discloses for a purpose beyond what's needed for processing for the transferor (s11(2))
- Introduces a private right of action

CHINA—OMNIBUS DATA PROTECTION LAW (PIPL)

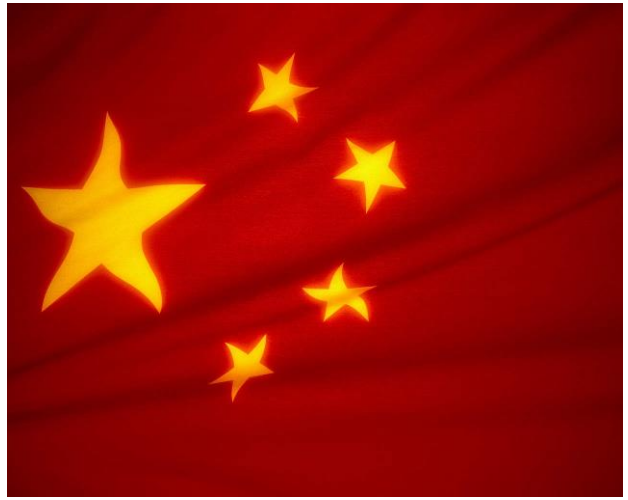
***Personal Information Protection Law* (PIPL) passed in November 2020:**

- China's first omnibus privacy legislation identifying individuals' data rights
- Similar to previous regulations passed in China, but this law grants enforcement rights to individuals
- Substantially similar to GDPR (e.g. rights of access, rights to rectification and erasure)



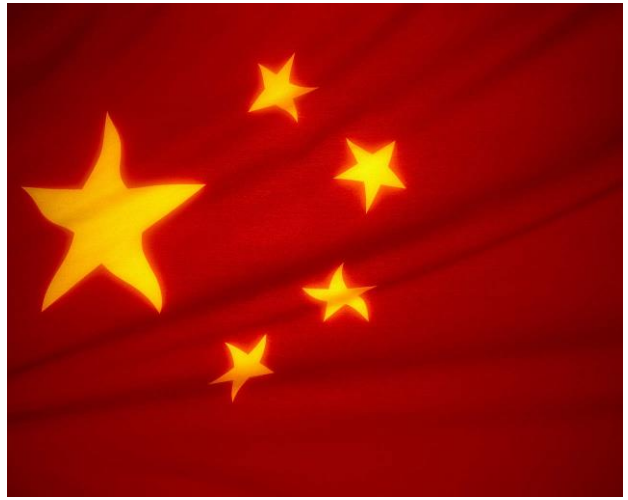
CHINA—OMNIBUS DATA PROTECTION LAW (PIPL)

- Will apply to all data processing in China
- Extraterritorial like GDPR for:
  - Provision of products / services to persons in China
  - Analysis of behaviour of persons in China
- Specific consent required to transfer personal data to third parties—must identify the recipient, purpose of transfer, type of data transferred, and method of processing



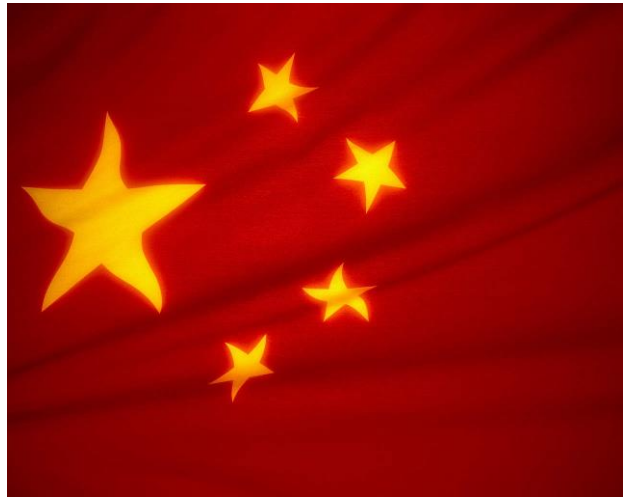
CHINA—OMNIBUS DATA PROTECTION LAW (PIPL)

- Under previous (extant) *Cyber Security Law* (CSL), regulatory approval required to transfer data overseas, but no process for obtaining permission exists
- PIPL implements GDPR-like structure with measures for network operators transferring data above a threshold level
- Below threshold, organizations can transfer data out of China if they (i) obtain a data protection certificate, (ii) enter into contract with recipient guaranteeing PIPL compliance, or (ii) pass a gov't security assessment



CHINA—OMNIBUS DATA PROTECTION LAW (PIPL)

- Above the data threshold level, transferring organizations must pass a government security assessment (no requirements / process in place yet)
- Regardless of threshold, transferor must obtain data subjects' consent to transfer
- Fines for breach of PPL by an organization up to RMB50,000,000 or 5% of its annual income
- Fines for breach by individual: mandatory minimum RMB 10,000, maximum of RMB100,000



RECOMMENDATIONS

- **Practical aspects on international data protections frameworks affecting you as general counsel for international businesses**

  1. Build data maps relevant to your business
  2. Prioritise risk regions
  3. Identify common/baseline compliance elements across jurisdictions
  4. Stay up-to-date with relevant global legal frameworks

QUESTIONS?

GOWLING WLG

CONTACT

BRENT J. ARNOLD

Partner, Advocacy

Technology Sub-Group Leader (Com Lit)

T +1 416 347 2737
brent.arnold@gowlingwlg.com

Brent J. Arnold is a partner practising in the Toronto office of Gowling WLG's Advocacy department, specializing in commercial litigation, data breach coaching and response, and data breach class action defence.

Brent is Vice Chair of the Steering Committee for the Cybersecurity and Data Privacy section of the U.S.-based Defence Research Institute (DRI), and sits on the executive of the Ontario Bar Association's Privacy and Access to Information Law Committee. He is corporate secretary for the Canadian chapter of the Internet Society, a global organization devoted to improving the affordability, accessibility, fairness and security of the internet.

Brent currently serves as a member of the court-appointed joint E-Hearings Task Force, whose mandate is to facilitate the modernization and re-opening of Ontario courts in the wake of the COVID-19 crisis.

GOWLING WLG

CONTACT

TODD BURKE

Partner

T +1 613-786-0226
todd.burke@gowlingwlg.com

Todd Burke practises in the areas of complex commercial litigation, insurance defence, professional liability and crisis management. With over 25 years in practice, Todd has represented national and international clients in a number of sectors, including manufacturing, finance, technology, transportation, health and nuclear energy.

In civil and arbitration mandates, he delivers effective representation, proven value and excellent client service. In a 2018 trade secret case, the judge commented that an expert "was largely destroyed" based on Todd's cross-examination. Recent mandates have focused on shareholder disputes, oppression claims, real estate disputes, software implementation, environmental contamination, construction disputes, professional negligence and disciplinary proceedings before various professional colleges.

Todd also has extensive experience in domestic and international arbitration, cross-border issues and in obtaining injunctions.

Given his broad experience, Todd is available to act as an arbitrator on cases in the commercial, insurance and professional liability fields.

GOWLING WLG

GOWLING WLG