

Data Privacy Update – Ensuring Compliance Amidst an Evolving Regulatory Landscape

Justine Kasznica and Ashleigh Krick

Agenda

- Recent Events: Why is this topic relevant?
- Overview of GDPR, CCPA, PIPEDA
- U.S. Landscape – Proposed State Legislation
- Practice Pointers & Best Practice



Recent Events

- International and Domestic Legislation
 - CCPA effective January 1, 2020
 - Privacy Shield Overturned July 16, 2020
- Enforcement
 - CCPA Enforcement began July 1, 2020
 - Increased Federal Trade Commission Activity.
 - Twitter Investigation
 - Facebook: \$5 Billion Dollar Penalty and Conduct Relief
- Evolving U.S. Landscape

Overview: GDPR, CCPA, PIPEDA

Overview

- EU's General Data Protection Regulation (GDPR)
- California's Consumer Privacy Act (CCPA)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

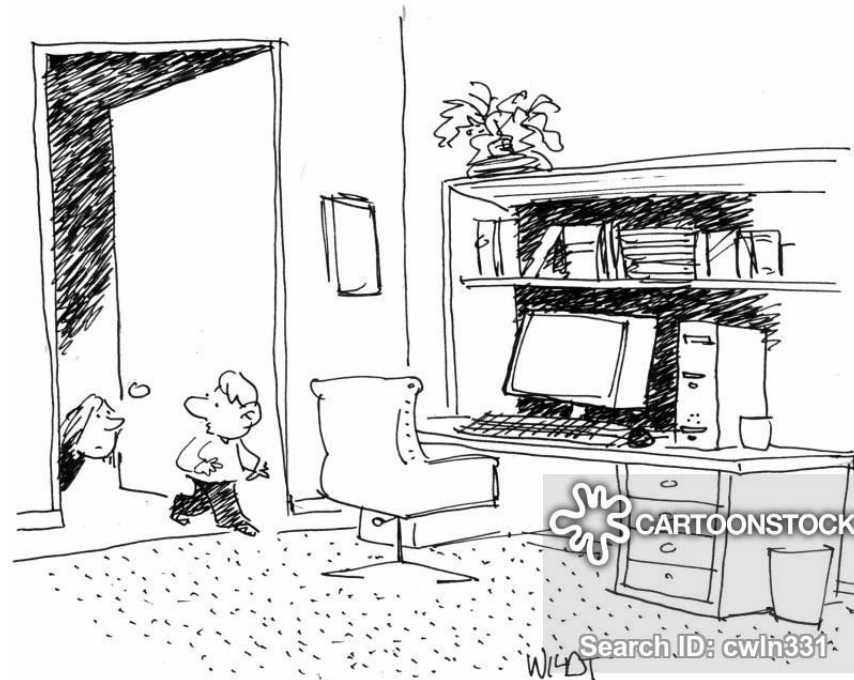
Overview

- Applicability criteria
- Notice of data collection
- Consumer rights
- Security and data breach notification
- Enforcement mechanisms

General Data Protection Regulation (GDPR) & Other European Legislation

European Law Updates

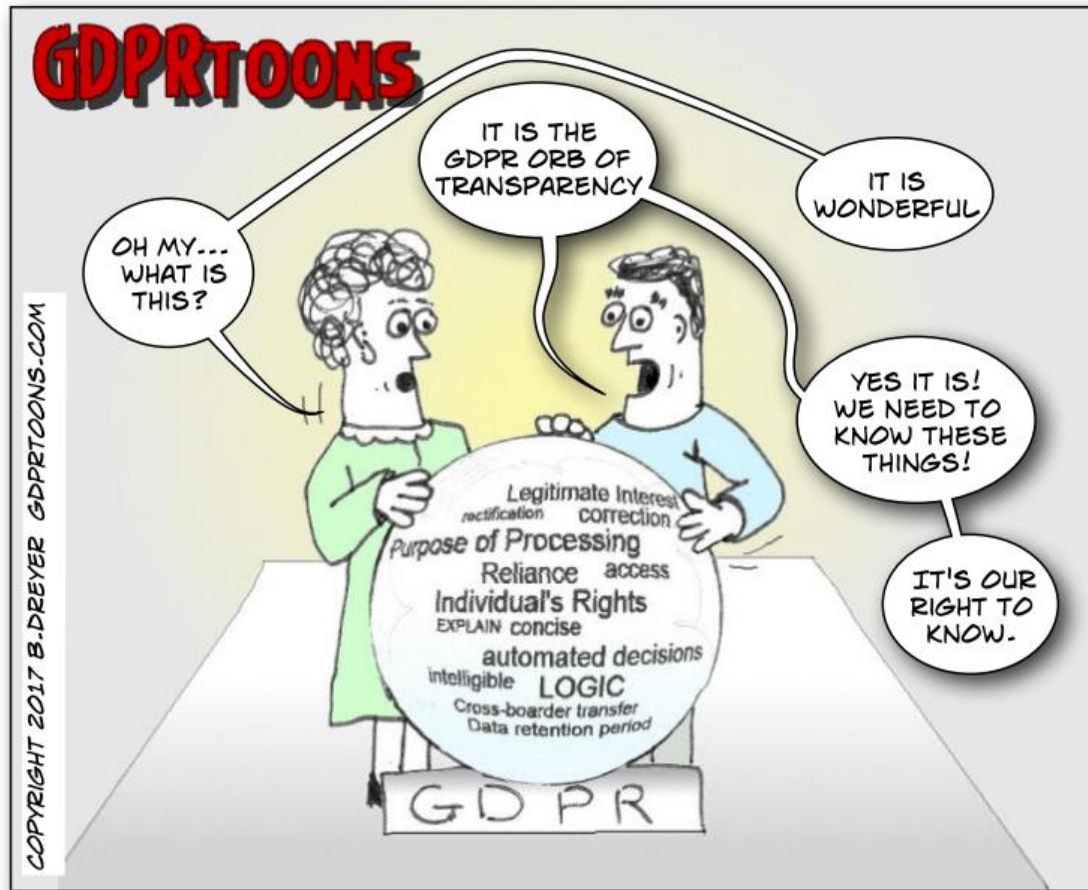
- EU-US Privacy Shield Overturned
- The ePrivacy Directive (cookie law)



"Shhhhh...they're in here somewhere. Dad's always talking about the cookies in his computer."

GDPR: Applicability

- Processing the personal data of data subjects



GDPR: Applicability

The GDPR applies to:

- Entity that processes personal data as part of its activities in the EU, regardless of where the data is processed
- or
- An entity established outside the EU that is either
 - offering goods/services (paid or for free)
 - or
 - is monitoring the behavior of individuals in the EU

GDPR



GDPR: Key Elements



GDPR Enforcement

GDPR Maximum Penalty:

**€20 million, or up to 4%
of the annual worldwide
turnover of the
preceding financial year,
whichever is greater.**

Major GDPR fine count:

- 2020: 17
- 2019: 31
- 2018: 1
- **Total: 49**

Major GDPR fine totals:

- 2020: € 77,958,722
- 2019: € 440,515,407
- 2018: € 400,000
- **Total: € 518,874,129**

GDPR Enforcement

- Most frequent violations
 - Data access/subject requests: Insufficient response to data subject/insufficient transferability measures
 - Lawful processing: Insufficient legal basis for data processing; Non-compliance with general data processing principles
 - Data breach: Insufficient technical and organizational measures to ensure information security
 - Transparency
 - Data Minimization

GDPR Enforcement

- Google: €50 million (\$56 million)
 - Art. 6, Consent and transparency, prechecked consent on personalized advertising
- Marriot: \$99M Pounds
 - Data breach affecting 30M EU residents; insufficient technical and organizational measures to ensure information security
- PwC: €150,000 (\$165,400)
 - Art. 83, violation of fairness and transparency principles on data use of employees for commercial purposes
- Other Investigations: Facebook, Instagram, Twitter, LinkedIn, Verizon, Apple, etc.

California Consumer Privacy Act (CCPA)

CCPA: Applicability

- Business that:
 - does business in the State of California,
 - collects personal information of California residents,
 - alone or with others determines the purposes or means of processing of that data, and
 - satisfies one or more of the following:
 - (i) annual gross revenue in excess of \$25 million,
 - (ii) alone or in combination, annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices, or
 - (iii) derives 50% or more of its annual revenues from selling consumers' personal information.

CCPA: Key Elements



CCPA: Enforcement

- Attorney General regulations went into effect on August 14, 2020 and began enforcement on July 1, 2020
- **Class Actions Filed under CCPA Private Right of Action (Zoom Case):** a consumer's personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.150(a)(1)

On Deck: California Privacy Law

- CA Privacy Rights Act (CPRA) – On November Ballot
 - Sensitive information
 - “Sale” Definition
 - Creation of enforcement agency: California Privacy Protection Agency

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA: Applicability

- Business that
 - collects, uses, or discloses
 - personal information of individuals residing in Canada
 - in the course of commercial activities in Canada

PIPEDA: Key Elements



U.S. Landscape

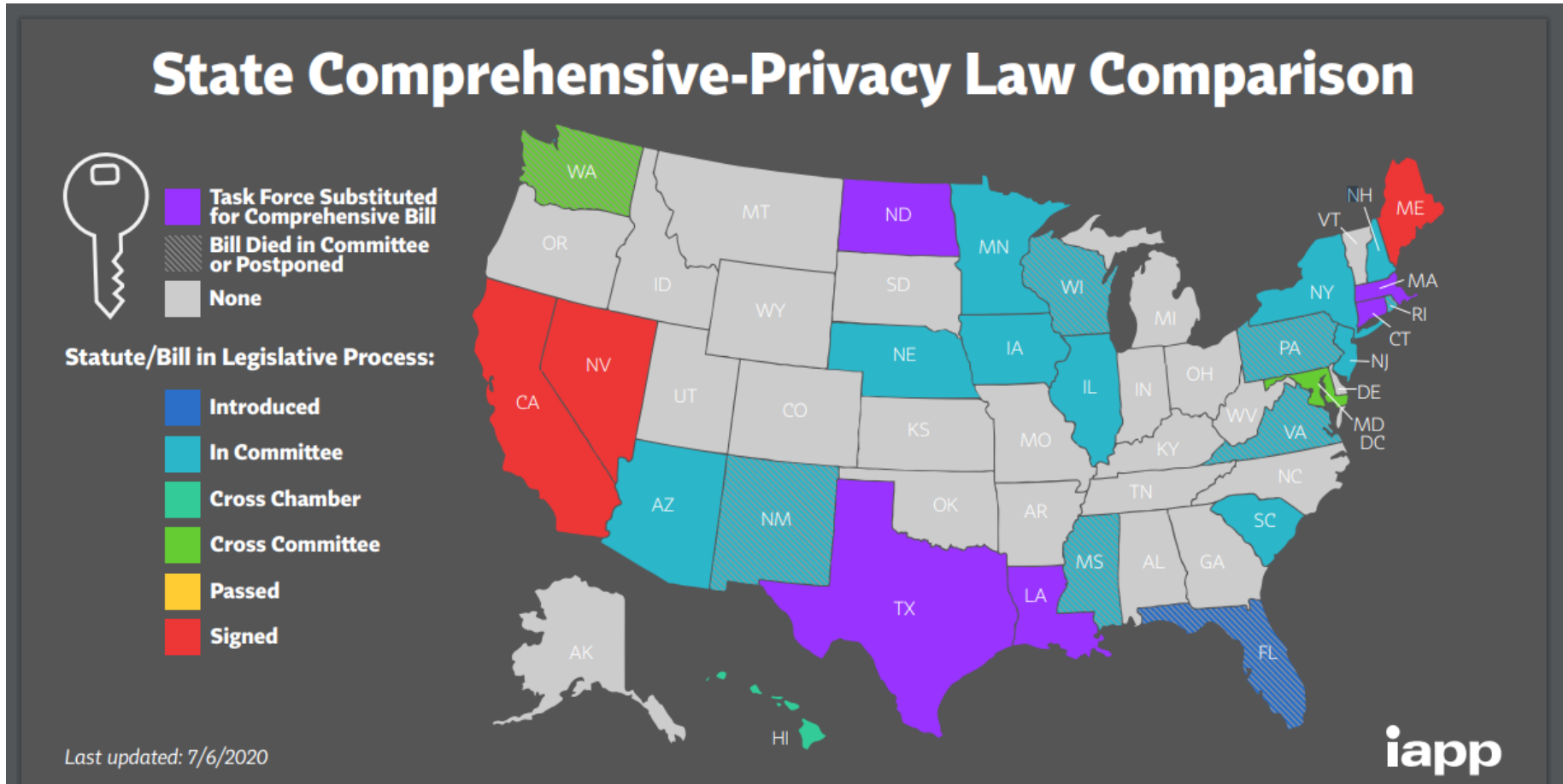
U.S. Federal Landscape

- **Privacy Act of 1974** — Protects personal information maintained by federal agencies
- **Health Insurance Portability and Accountability Act (HIPAA) / Health Information Technology for Economic and Clinical Health Act (HITECH)** — Protects personal health information (PHI)
- **Gramm–Leach–Bliley Act (GLBA)**— Protects financial information
- **Children’s Online Privacy Protection Act (COPPA)** — Protects children’s privacy
- **Family Educational Rights and Privacy Act (FERPA)** — Protects students’ personal information
- **Fair Credit Reporting Act (FCRA)** — Governs the collection and use of consumer information

U.S. Federal Landscape

- **FTC Enforcement** - Legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury.
 - Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce
 - Enforcement of other federal laws relating to consumers' privacy and security.
- **Twitter Investigation**

U.S. State Law Landscape



U.S. State Law Landscape

- Consumer Privacy
 - Illinois Biometric Privacy Act (BIPA)
 - Nevada SB 220 (October 1, 2019)
 - Maine Act to Protect the Privacy of Online Customer Information (July 1, 2019)
 - Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (March 1, 2010)
 - New York Consumer Privacy Act (NYPA) (Pending)
- Data Breach Notification Laws

U.S. Case Law

- *Dittman v. UPMC* (PA 2018)



"You may want to look into getting a better cybersecurity system. I don't think that sign will be enough."

Practice Pointers & Best Practices

“Privacy by Design”

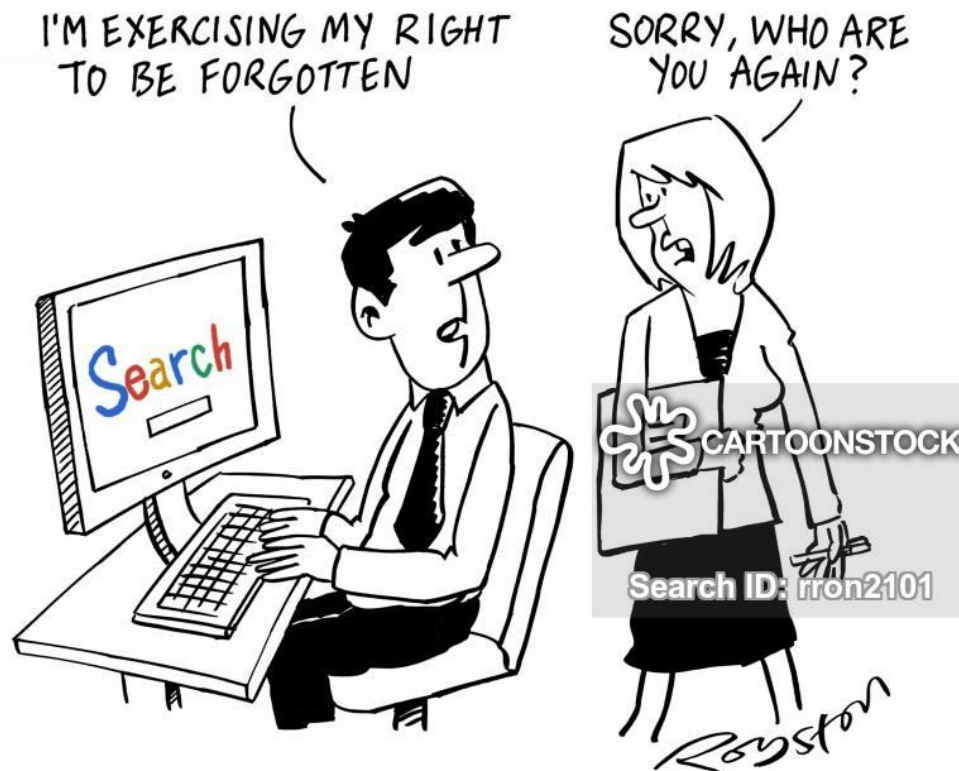
- Data Privacy POC/DPO
- Privacy Impact Assessment (PIA)
- Compliance Obligations
- Design and Implementation

Make sure you have an updated, compliant Privacy Policy.



"Can't say. It's private."

Prepare for responding to a consumer request under GDPR, CCPA, or PIPEDA.



Q&A

- Q#1: Differences in Approach Between B2B and B2C Businesses

Q#2: Practical Pointers Post-Privacy Shield World;
SCCs

Q#3: Restrictions on electronic devices when
traveling abroad

- Other Questions?



Thank you!

Justine Kasznica

412.394.6466

jkasznica@babstcalland.com

Ashleigh Krick

202.853.3466

akrick@babstcalland.com

Where Trust and Value Meet™

**Construction | Corporate and Commercial | Creditors' Rights and Insolvency | Emerging Technologies
Employment and Labor | Energy and Natural Resources | Environmental | Litigation
Public Sector | Real Estate | Transportation Safety**

Pittsburgh, PA | Charleston, WV | Houston, TX | Sewell, NJ | State College, PA | Washington, DC

babstcalland.com

Copyright © 2020 Babst, Calland, Clements and Zomnir, P.C.