How to Stay Compliant with the Changing Global Privacy and Data Security Laws

July 10, 2018

Melissa Krasnow
VLP Law Group LLP, Minneapolis
Email: mkrasnow@vlplawgroup.com
Attorney biography:
https://www.vlplawgroup.com/attorneys/melissa-krasnow/

With thanks to the following for their helpful comments on these slides:

European Union slides:

Vinod Bange, Taylor Wessing, London
Email: v.bange@taylorwessing.com

Canada slides:

Wendy Mee, Blake, Cassels & Graydon, Toronto
Email: wendy.mee@blakes.com

BUSINESS & REAL ESTATE

California now world's fifth-largest economy, bigger than Britain

BY BENJY EGEL
begel@sacbee.com

May 04, 2018 10:01 AM
Updated May 04, 2018 03:44 PM

The Golden State is getting even richer.

California is now the world's fifth-largest economy, according to data released Friday morning by the U.S. Department of Commerce. Its 2017 Gross State Product was $2.747 trillion, surpassing the United Kingdom's $2.625 trillion Gross Domestic Product.

The new ranking marks the highest point for California's relative GSP since 2002. The state had slipped to the 10th-largest world economy in 2012, when its GSP was just $2.003 trillion.

Texas was the U.S.'s next highest-producing state with a GSP of $1.696 trillion, followed by New York, Florida and Illinois. Vermont, Wyoming and Montana produced the least valuable goods and service in the U.S.

estate loaded with awesome amenities

VIEW MORE VIDEO

MORE BUSINESS & REAL ESTATE

Distracted driving, other laws set to take effect Sunday

Trump claims Saudi Arabia will boost oil production

Louisiana sales tax rate changes Sunday, part of budget deal

New laws set to go into effect in Virginia

Opioid measures among new Tennessee laws kicking in

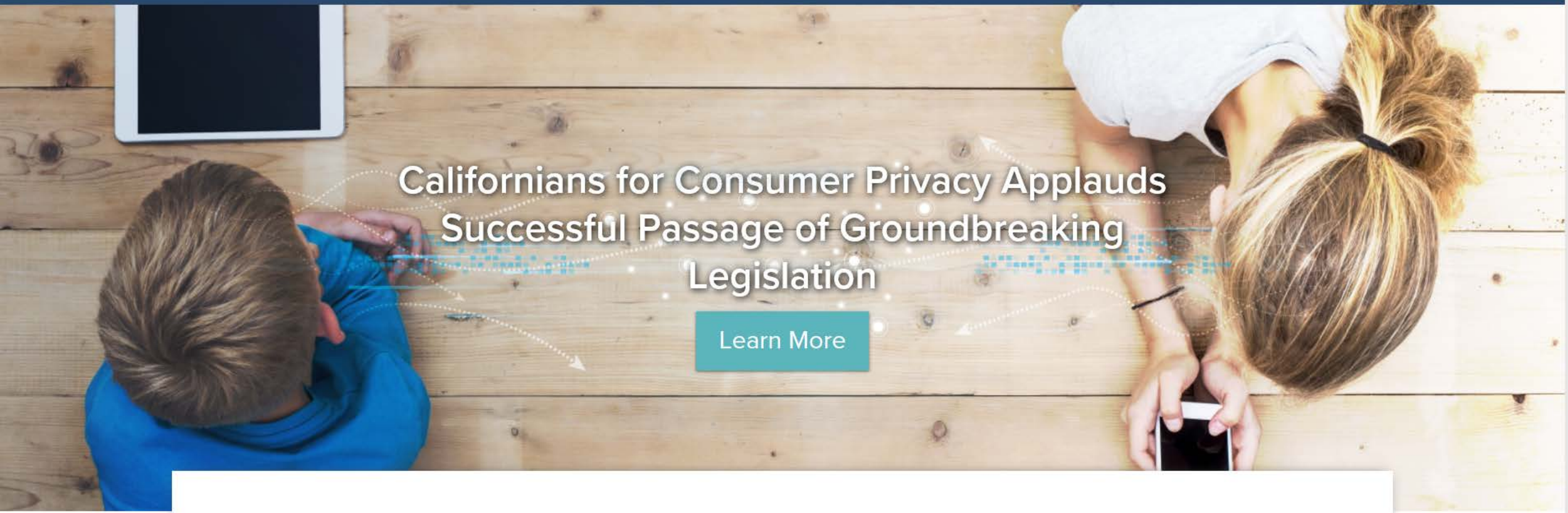
MORE BUSINESS & REAL ESTATE

Home | California Consu

caprivacy.org

CALIFORNIA CONSUMER PRIVACY ACT

About Facts Updates Coalition Contact Donate



First-in-the-nation consumer privacy rights are the law of the land in California!

8:41 AM
6/30/2018

AB-375 Privacy: personal information: businesses. (2017-2018)

Date Published: 06/29/2018 04:00 AM

Assembly Bill No. 375

CHAPTER 55

An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.

[Approved by Governor June 28, 2018. Filed with Secretary of State June 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 375, Chau. Privacy: personal information: businesses.

The California Constitution grants a right of privacy. Existing law provides for the confidentiality of personal information in various contexts and requires a business or person that suffers a breach of security of computerized data that includes personal information, as defined, to disclose that breach, as specified.

This bill would enact the California Consumer Privacy Act of 2018. Beginning January 1, 2020, the bill would grant a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared. The bill would

European Union

GDPR IN EFFECT

- European Union's (EU's) General Data Protection Regulation went into effect May 25, 2018 and applies to data controllers and data processors

- See text of GDPR at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

GDPR DEFINITIONS (ARTICLE 4)

- Data controller: a person, which, alone or jointly with others, determines the purposes and means of the processing of personal data

- Data processor: a person that processes personal data on behalf of data controller

- Data subject: a natural person to whom the personal data relates

- Personal data: any information that relates to an identified or identifiable living individual

- Personal data breach: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Processing: any operation performed on personal data

WHEN GDPR APPLIES (ARTICLE 3)

GDPR applies where data controller or data processor:

- has an establishment in the EU and processes personal data, regardless of whether the processing takes place in the EU

- is not established in the EU and processes personal data of data subjects who are in the EU, where the processing activities relate to (i) offering goods or services to such data subjects in the EU, whether for payment or for free, or (ii) monitoring their behavior within the EU

- See: https://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-authors-international-risk-management-institute-article-application-eus-general-data-protection-regulation/

DATA CONTROLLER AND DATA PROCESSOR OBLIGATIONS UNDER GDPR

- See: https://globaldatahub.taylorwessing.com/article/data-controller-requirements-under-gdpr

- See: https://globaldatahub.taylorwessing.com/article/data-processor-obligations-under-the-gdpr

DATA CONTROLLER OBLIGATIONS:
REQUIRED PRIVACY NOTICE CONTENT (ARTICLES 12-22)

- identity and contact details and, where applicable, data controller's representative
- contact details of data protection officer, where applicable
- purposes of processing for which personal data are intended and legal basis for processing
- where processing is based on legitimate interests, description of legitimate interests pursued by data controller or by third party
- categories of personal data

DATA CONTROLLER OBLIGATIONS:
REQUIRED PRIVACY NOTICE CONTENT (ARTICLES 12-22) (CON'T)

- source from which personal data originate, and if applicable, whether it came from publicly accessible sources

- whether provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether data subject is obliged to provide personal data and the possible consequences of failure to provide such data

- recipients or categories of recipients of the personal data, if any

- period for which the personal data will be stored, or if not possible, the criteria used to determine that period

DATA CONTROLLER OBLIGATIONS:
REQUIRED PRIVACY NOTICE CONTENT (ARTICLES 12-22) (CON'T)

- existence of the right to request from data controller access to and rectification or erasure of personal data or restriction of processing concerning data subject or to object to processing and the right to data portability

- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal

- right to lodge a complaint with a supervisory authority

DATA CONTROLLER OBLIGATIONS:
REQUIRED PRIVACY NOTICE CONTENT (ARTICLES 12-22) (CON'T)

- existence of automated decision-making, including profiling and meaningful information about the logic involved, and the significance and the envisaged consequences of such processing for data subject

- that data controller intends to transfer personal data outside of the EU and description of safeguards relied upon and the means to obtain copies of transfer agreements

- See: https://edpb.europa.eu/node/66

DATA PROCESSOR AND DATA CONTROLLER OBLIGATIONS: BREACH NOTIFICATION (ARTICLES 32-34)

- Data processor must notify data controller without undue delay after becoming aware of a personal data breach

- Data controller must notify the competent supervisory authority of a personal data breach without undue delay and where feasible not less than 72 hours after data controller becomes aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

- Data controller must communicate the personal data breach to data subjects without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and data controller has not either:
(i) implemented appropriate technical and organizational protection measures which were applied to the personal data affected by the personal data breach and render the personal data unintelligible to any person who is not authorized to access it (e.g., encryption) or (ii) taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize

DATA PROCESSOR AND DATA CONTROLLER OBLIGATIONS: BREACH NOTIFICATION (ARTICLES 32-34) (CON'T)

- Where such communication of the personal data breach to data subjects would involve disproportionate effort, there instead shall be a public communication or similar measure whereby data subjects are informed in an equally effective manner

- See: https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_en

- See also: https://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-authors-primer-personal-data-breach-reporting-european-unions-general-data-protection-regulation-bloomberg-law/

TRANSFER OF PERSONAL DATA OUTSIDE OF EU (ARTICLES 44-50)

Safeguards for transfer of personal data outside of the EU include, without limitation:

- Model contracts
- See: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
- EU-US Privacy Shield - only covers transfers to the US
- See: https://www.privacyshield.gov/welcome

TRANSFER OF PERSONAL DATA OUTSIDE OF EU (ARTICLES 44-50) (CON'T)

- Binding corporate rules
- See: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en
- Adequacy decision regarding jurisdiction
- See: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

GDPR ENFORCEMENT (ARTICLES 77-84)

- Supervisory authorities can issue fines up to 4% of annual worldwide turnover or €20 million and have other powers (e.g., audit, issuing warnings and issuing temporary and permanent bans on processing)
- Individuals have a right to bring a claim against data controller or data processor in court

EPRIVACY REGULATION – NOT FINALIZED

- See: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Canada

CANADIAN PRIVATE SECTOR PRIVACY LAWS

- Canada has a comprehensive federal private sector privacy statute and provincial private sector privacy statutes

- General principle: consent to collect, use or disclose personal information is generally required (with certain exceptions)

- Also, the collecting, using and disclosing of that information must be for purposes that a reasonable person would consider appropriate in the circumstances, regardless of whether the individual has consented to the collection, use or disclosure of their personal information

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

- PIPEDA generally applies to all collection, use or disclosure of personal information by organizations in commercial activity

- PIPEDA defines personal information broadly, including any information about an identifiable individual, whether public or private, with certain exceptions

- PIPEDA does not apply to the collection, use and disclosure of employee information by provincially regulated private sector employers (i.e., most organizations)

- Federally regulated employers (e.g., banks, airlines, telecommunication companies, etc.) are covered, but most Canadian companies are provincially regulated

- Organizations are exempt from PIPEDA regarding activities covered by the substantially similar provincial laws if the activity takes place wholly within a province; however cross-border (i.e., provincial/national) activities remain subject to PIPEDA

CANADIAN BILL S-4 (DIGITAL PRIVACY ACT) AMENDED PIPEDA

- Individual consent is valid if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which the individual is consenting

- Certain exceptions to consent requirement

- "Business transaction" exemption: organizations can use and disclose personal information without consent in connection with mergers, acquisitions, financings, etc. (both during due diligence and post-closing) where certain conditions are met

- Business contact information is defined more broadly (includes business email addresses) and is not excluded from the definition of personal information. However, PIPEDA's personal information provisions will not apply to the collection, use and disclosure of business contact information by an organization solely for the purpose of communicating with an individual about their employment, business or profession

- Canadian Privacy Commissioner authority to enter into compliance agreements with organizations reasonably believed to have violated or that are about to violate PIPEDA

EFFECTIVE NOVEMBER 1, 2018: MANDATORY BREACH NOTIFICATION

- See Breach of Security Safeguards Regulations at: http://www.gazette.gc.ca/rp-pr/p2/2018/2018-04-18/pdf/g2-15208.pdf

- See also: http://www.blakesbusinessclass.com/federal-data-breach-reporting-regulations-published-take-effect-november-2018/

- Mandatory breach notification as soon as feasible where "real risk of significant harm" to Canadian Privacy Commissioner and affected individuals

- Notification where appropriate to any third party that may be able to mitigate harm to affected individuals

- Required organizational maintenance of record of each breach, including where no "real risk of significant harm"

- Enforcement for non-compliance

CANADIAN PRIVACY COMMISSIONER GUIDANCE UNDER PIPEPA

- See: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180524/
- Effective July 1, 2018: inappropriate data practices
- Effective January 1, 2019: meaningful consent

RECENTLY INTRODUCED LEGISLATION TO AMEND PIPEDA (BILL C-413)

- See: http://www.parl.ca/Content/Bills/421/Private/C-413/C-413_1/C-413_1.PDF

- Would expand the grounds where Canadian Privacy Commissioner may decide not to investigate a complaint

- Would authorize Canadian Privacy Commissioner to make orders directing an organization to take any action that, in Canadian Privacy Commissioner's opinion, is reasonable to ensure compliance with the organization's obligations under PIPEDA

- Would provide for offenses punishable by fines of up to C$30 million where an organization is found not to comply with certain obligations under PIPEDA

COMPREHENSIVE PROVINCIAL PRIVATE SECTOR PRIVACY LAWS

- Alberta, British Columbia and Quebec have comprehensive private sector privacy laws

- Manitoba adopted a comprehensive private sector privacy law (but unclear whether or when it will be proclaimed into force)

- Other provinces have more limited privacy legislation, for example, dealing with health information

- These provincial comprehensive sector privacy laws apply to organizations collecting, using or disclosing personal information within a province where the province has enacted legislation that is substantially similar to PIPEDA

CANADIAN PRIVATE SECTOR PRIVACY LAWS - DATA BREACH NOTIFICATION

- Alberta – must notify Alberta Privacy Commissioner, which can direct notification to affected individuals

- Manitoba – must notify affected individuals (unclear whether or when it will be proclaimed into force)

- Canadian Privacy Commissioner – voluntary privacy breach guidelines are **currently in force**

- Federal and provincial privacy commissioners have also published guidelines that are **currently in force** that suggest disclosure and notification should be made in certain circumstances

CANADA'S ANTI-SPAM LAW (CASL)

- See https://crtc.gc.ca/eng/internet/anti.htm

- Applies to all commercial electronic messages (CEMs), including email, text messages, instant messages and social networking communications sent to an electronic account (e.g., direct messages, but not posts) where the computer system used to send or access the CEM is located in Canada, unless the CEM is subject to an exception

- Cannot send a CEM unless the recipient consented to its receipt and the message meets certain form and content requirements

- Cannot install computer programs on another person's computer without express prior consent

CASL ENFORCEMENT / ACTIONS

- Significant administrative monetary penalties
- Liability for senders, those who cause sending and those who aid, induce or procure sending of prohibited CEMs
- Vicarious liability for directors, officers and employers for noncompliance with CASL, subject to a due diligence defense
- **Indefinitely suspended and not in force:** violation of CASL also can be the subject of a private right of action by any affected individual or organization